KESSLER TOPAZ
MELTZER & CHECK, LLP
JENNIFER L. JOOST (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Tel: (415) 400-3000
Fax: (415) 400-3001

-and-

JOSEPH H. MELTZER (*Pro Hac Vice*)
jmeltzer@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610) 667-7056

ROBBINS GELLER RUDMAN
& DOWD LLP
ROBERT M. ROTHMAN (*Pro Hac Vice*)
rrothman@rgrdlaw.com
58 South Service Road, Suite 2000
Melville, NY 11747
Tel: (631) 367-7100
Fax: (631) 367-1173

-and-

STUART A. DAVIDSON (*Pro Hac Vice*)
sdavidson@rgrdlaw.com
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Tel: (561) 750-3000
Fax: (561) 750-3364

Interim Co-Lead Counsel for Plaintiffs and the Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DIANA HAUCK, et al., Plaintiffs, v. ADVANCED MICRO DEVICES, INC., Defendant.	Civil Action No. 18-CV-00447-LHK **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

Plaintiffs Diana Hauck, Shon Elliott, Michael Garcia, JoAnn Martinelli, Benjamin D. Pollack, and Jonathan Caskey-Medina (collectively "Plaintiffs"), individually, and on behalf of all others similarly situated, hereby allege the following based on personal knowledge as their own conduct, and upon information and belief as to all other matters.

I. INTRODUCTION

1. This case concerns Defendant Advanced Micro Devices, Inc.'s ("Defendant," "AMD," or the "Company") violations of state common law and state and federal statutory law with respect to the manufacture and sale of defective central processing units ("CPUs" or "processors") to the Plaintiffs and the Classes (as defined herein). Consumers purchased AMD processors because of their advertised speed, performance, and security. In order to reach advertised levels of performance, AMD designed and engineered the microarchitecture of its CPUs to rely upon branch prediction, speculative execution, and caches.

2. However, unbeknownst to Plaintiffs and the Classes (defined herein), as designed and engineered by AMD, each of these processes can be infiltrated and coerced by a malicious attacker to leak data about consumers' sensitive information which, when analyzed by the attacker, can reveal the sensitive information itself (the "Defect"). *See infra* Section IV.C.1.

3. Because the attacker artificially triggers a natural function of AMD's CPU caches, and branch prediction and speculative execution processes (e.g., cache misses or conflicts, branch analysis, exceptions, and mis-speculation) and utilizes a "side-channel" to siphon out the targeted data, neither the CPU nor the consumer are aware that the CPU's microarchitecture has been compromised. Moreover, these attacks cannot be prevented by, among other things, anti-virus software because they take advantage of an inherent design defect in the hardware itself. This Defect was the result of AMD's decision to compromise the confidentiality of consumers' most sensitive information to increase the speed and performance levels of its CPUs. In short, AMD sacrificed security for speed.

4. Consumers, including Plaintiffs, purchased AMD CPUs or computing devices powered by AMD CPUs without the knowledge that AMD had sacrificed the security of their sensitive information to meet speed and performance benchmarks. In particular, Plaintiffs and the

Classes were unaware that, as designed and engineered by AMD, the CPU's microarchitecture exposed consumers' sensitive information to unauthorized access by a malicious attacker, and that, as designed by AMD, the CPU could not reach advertised performance specifications without the Defect. *See infra* Sections II.A.1-6; IV.B. More specifically, consumers purchased AMD CPUs or a computing device powered by an AMD CPU without knowing that, as designed by AMD, the CPU's caches, and branch prediction and speculative execution processes left consumers' sensitive information exposed. *See infra* Sections IV.B.2-4. Consumers likewise were unaware at the time of their purchase that the risk the Defect posed to their sensitive information was heightened when they engaged in "cloud" computing and, critically, was not addressed by any of the security technology AMD touted in its marketing. *See infra* Sections IV.B.5.

5. AMD, on the other hand, has been aware since at least 2003 that attackers could take advantage of the natural processes of the Company's CPU microarchitecture design to leak data about consumers' sensitive information. Specifically, AMD was aware no later than 2003 and certainly by 2007 that "[t]he internal functions of some microprocessor components like data and instruction caches and branch prediction units cause very serious side-channel leakage and hence create crucial security risks." AMD also was aware that the Defect could be exploited by attacks that were an "extremely attractive . . . weapon in the attacker's arsenal" because they were "easy to perform," and "[t]he attacker can achieve his goal by acting like a normal process, performing a legitimate operation." *See infra* Section IV.C.2.b.

6. Likewise, since 2009 and certainly by 2013, AMD has been aware that attackers could successfully manipulate physical microarchitectural resources (e.g., CPU caches) that are shared by consumers engaged in cloud computing to learn otherwise confidential information. *See infra* Section IV.C.2.c. These attacks were considerably more dangerous and powerful than previously disclosed microarchitectural attacks because they allowed an attacker to spy on consumers' sensitive information from a remote location. Accordingly, AMD knew the relevant computing usage scenarios, the security problem to be addressed, and the threat model attackers would utilize, and was able to address the Defect through a secure hardware design that provided

sufficient mechanisms to protect consumers' sensitive information from microarchitectural attacks well before Plaintiffs and the Classes purchased their defective CPUs. *See infra* Section IV.C.2.

7. Yet, despite its knowledge of practical microarchitectural attacks, its public commitment to "secure" hardware design, and its knowledge of solutions to address the Defect, AMD did nothing to address the Defect prior to its public disclosure in January 2018. *See infra* Section IV.C.2.d. And, while *ad hoc* solutions have been proposed for some of the known exploits, including, for instance, ensuring that data regarding Advanced Encryption Standard ("AES") keys is never stored in the CPUs' caches and releasing "patches" meant to address certain aspects of a set of exploits publicly disclosed in January 2018, AMD has not yet fixed the Defect inherent in its CPUs. *See infra* Section IV.D.

II. PARTIES

A. Plaintiffs

1. Diana Hauck

8. Plaintiff Diana Hauck is a resident and citizen of the State of Louisiana. On November 4, 2016, Ms. Hauck purchased an HP 15-ba079dc Notebook computer, containing an AMD A10-9600P processor, for $349.99, at the Best Buy in Metairie, Louisiana located at 6205 Veterans Boulevard. Ms. Hauck purchased her computer for personal computing, including checking email and drafting Excel spreadsheets.

9. The AMD processor's specifications, including its clock speed or frequency, were prominently displayed next to an in-store sample of the computer Ms. Hauck purchased. Ms. Hauck reviewed the specification representing that the speed of the AMD A10-9600P processor was 2.4 GHz with a max boost speed of 3.3 GHz and relied upon that stated speed in making the decision to purchase the computer.

10. Unbeknownst to Ms. Hauck, but known to AMD well before Ms. Hauck's purchase date, the AMD A10-9600P processor utilized a defective microarchitecture design that allowed an attacker to infiltrate and coerce the processor's caches, as well as its branch prediction and speculative execution processes, to leak data about Ms. Hauck's most sensitive information. After learning of the Defect in January 2018, Ms. Hauck installed a "patch" that purportedly mitigated the

risk to her sensitive information presented by the Defect. However, the patch failed to cure the Defect. Moreover, once the patch was applied to her computer, Ms. Hauck's processor no longer could achieve its advertised performance level, and her computer frequently crashed, sometimes several times per day.

11. At the time of her purchase, Ms. Hauck relied on AMD's representations that the AMD processor would perform as advertised and was not defective. Ms. Hauck was unaware at the time of her purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to her sensitive information; (iii) the AMD CPU that powered her computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of her sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered her computer to reach the advertised performance level. Had Ms. Hauck been aware of these facts, she would not have purchased the computer, or paid substantially less for the computer.

2. Shon Elliott

12. Plaintiff Shon Elliott is a resident and citizen of the State of California. Mr. Elliott is a longtime customer of AMD processors. Between 2005 and 2016, Mr. Elliott purchased several AMD processors, four of which are in computers or servers. On April 21, 2016, Mr. Elliott purchased an AMD FX-8370 processor with Wraith cooler, for $157.50, at the Fry's Electronics ("Fry's") in Sunnyvale, California. Mr. Elliott purchased the processor to install in a computer he used primarily for his audio/video production and IT consulting business, as well as some personal computing. Specifically, he needed a processor which could smoothly handle video editing and video rendering.

13. The AMD processor's specifications, including its clock speed or frequency, were prominently displayed on the box of the CPU Mr. Elliott purchased, as well as on the receipt reflecting Mr. Elliott's purchase. Mr. Elliott reviewed the specification representing that the speed of the AMD FX-8370 processor was 4.0 GHz with a max boost speed of 4.3 GHz and relied upon that stated speed in making the decision to purchase the processor.

EXHIBIT 1

14. Unbeknownst to Mr. Elliott, but known to AMD well before Mr. Elliott's purchase date, the AMD FX-8370 processor utilized a defective microarchitecture design that allowed an attacker to infiltrate and coerce the processor's caches, as well as its branch prediction and speculative execution processes, to leak data about Mr. Elliott's most sensitive information. After learning of the Defect in January 2018, Mr. Elliott installed a "patch" that purportedly mitigated the risk to his sensitive information presented by the Defect. However, the patch failed to cure the Defect. Moreover, once the patch was applied to Mr. Elliott's AMD FX-8370 processor, his processor could no longer achieve its advertised performance level and his computer ran more slowly. Now that he is aware of the Defect, Mr. Elliott runs more active checks of his system security, and does more security checks of his computer, which takes at least two hours each week.

15. At the time of his purchase, Mr. Elliott relied on AMD's representations that the AMD processor would perform as advertised and was not defective. Mr. Elliott was unaware at the time of his purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to his sensitive information; (iii) the AMD CPU that powered his computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of his sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered his computer to reach the advertised performance level. Had Mr. Elliott been aware of these facts, he would not have purchased his processor, or paid substantially less for his processor.

3. Michael Garcia

16. Plaintiff Michael Garcia is a resident and citizen of the State of California. On April 21, 2016, Mr. Garcia purchased an AMD FX-8370 processor with Wraith cooler at Fry's in Sunnyvale, California. Mr. Garcia purchased the processor to install in a personal computer, which he used for document, audio, video, and graphics editing. He also needed a processor that could handle transcoding data for multiple users at the same time.

17. The AMD processor's specifications, including its clock speed or frequency, were prominently displayed on the box and on the receipt. Mr. Garcia reviewed the specification

EXHIBIT 1
Page 7 of 123

representing that the speed of the AMD FX-8370 processor was 4.0 GHz with a max boost speed of 4.3 GHz and relied upon that stated speed in making the decision to purchase the processor.

18. Unbeknownst to Mr. Garcia, but known to AMD well before Mr. Garcia's purchase date, the AMD FX-8370 processor utilized a defective microarchitecture design that allowed an attacker to infiltrate and coerce the processor's caches, as well as its branch prediction and speculative execution processes, to leak data about Mr. Garcia's most sensitive information. After learning of the Defect in January 2018, Mr. Garcia installed a "patch" that purportedly mitigated the risk to his sensitive information presented by the Defect. However, the patch failed to cure the Defect. Moreover, once the patch was applied to Mr. Garcia's AMD FX-8370 processor, his processor could no longer achieve its advertised performance level and he noticed a pronounced performance decrease. The computer ran more slowly and would "chug" when performing graphic and video editing, and could only transcode data for one user at a time. As a result of the Defect and the performance decrease he experienced, Mr. Garcia no longer uses the processor.

19. At the time of his purchase, Mr. Garcia relied on AMD's representations that the AMD processor would perform as advertised and was not defective. Mr. Garcia was unaware at the time of his purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to his sensitive information; (iii) the AMD CPU that powered his computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of his sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered his computer to reach the advertised performance level. Had Mr. Garcia been aware of these facts, he would not have purchased his processor, or paid substantially less for his processor.

4. Joann Martinelli

20. Plaintiff Joann Martinelli is a resident and citizen of the State of California. On July 6, 2013, Ms. Martinelli purchased an HP Pavilion p7-1534, containing an AMD A8-5500 processor, for $532.11 at a Best Buy in Auburn, California, located at 1760 Grass Valley Highway. Ms.

Martinelli purchased the computer for personal computing, primarily emailing and communicating with family.

21. The AMD processor's specifications, including its clock speed or frequency, were prominently displayed next to an in-store sample of the computer. Ms. Martinelli reviewed the specification representing that the speed of the processor was 3.2 GHz with a max boost speed of 3.7 GHz and relied upon that stated speed in making the decision to purchase the processor.

22. Unbeknownst to Ms. Martinelli, but known to AMD well before Ms. Martinelli's purchase date, the AMD A8-5500 processor utilized a defective microarchitecture design that allowed an attacker to infiltrate and coerce the processor's caches, as well as its branch prediction and speculative execution processes, to leak data about Ms. Martinelli's most sensitive information. After learning of the Defect in January 2018, Ms. Martinelli installed a "patch" that purportedly mitigated the risk to her sensitive information presented by the Defect. However, the patch failed to cure the Defect. Moreover, once the patch was applied to Ms. Martinelli's AMD A8-5500 processor, the processor could no longer achieve its advertised performance level, and her computer ran more slowly and frequently froze, requiring reboots. As a result of the Defect and performance decreased she experienced with her computer, she avoids using her computer for any intensive tasks and decreased her use of the computer from every day to twice a week.

23. At the time of her purchase, Ms. Martinelli relied on AMD's representations that the AMD processor would perform as advertised and was not defective. Ms. Martinelli was unaware at the time of her purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to her sensitive information; (iii) the AMD CPU that powered her computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of her sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered her computer to reach the advertised performance level. Had Ms. Martinelli been aware of these facts, she would not have purchased the computer, or paid substantially less for her computer.

5. Benjamin D. Pollack

24. Plaintiff Benjamin D. Pollack is a resident and citizen of the State of Florida. On September 26, 2014, Mr. Pollack purchased an AMD A10-7850K processor, $179.99, for his personal computer on Newegg.com. Mr. Pollack purchased the processor to install in a personal computer, which he used for home productivity, such as using Microsoft Office, and for gaming, specifically massive multiplayer online games and large scale simulation games.

25. The AMD processor's specifications, including its clock speed or frequency, were prominently displayed on the webpage where he added the processor to his shopping cart, on the receipt, and on the box which he later received. Mr. Pollack reviewed the specification representing that the speed of the processor was 3.7 GHz with a max boost speed of 4.0 GHz and relied upon that stated speed in making the decision to purchase the processor.

26. Unbeknownst to Mr. Pollack, but known to AMD well before Mr. Pollack's purchase date, the AMD A10-7850K processor utilized a defective microarchitecture design that allowed an attacker to infiltrate and coerce the processor's caches, as well as its branch prediction and speculative execution processes, to leak data about Mr. Pollack's most sensitive information. After learning of the Defect in January 2018, Mr. Pollack installed a "patch" that purportedly mitigated the risk to his sensitive information presented by the Defect. However, the patch failed to cure the Defect.

27. Moreover, once the patch was applied to Mr. Pollack's AMD A10-7850K processor, his processor could no longer achieve its advertised performance level, and his computer system experienced more instability, crashing more often and needing more frequent reboots. The crashes typically came when he was playing the graphics-heavy games he purchased the processor to play and when he was watching Netflix video in the web browser. Once he became aware of the Defect, Mr. Pollack doubled up on his anti-virus software and increased his security settings. As a result of the Defect and the performance decrease he experienced, Mr. Pollack at first stopped using his computer for gaming and later ceased to use the processor altogether.

28. At the time of his purchase, Mr. Pollack relied on AMD's representations that the AMD processor would perform as advertised and was not defective. Mr. Pollack was unaware at

the time of his purchase that (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to his sensitive information; (iii) the AMD CPU that powered his computer could not reach the advertised performance without relying on defectively designed CPU microarchitecture components that compromised the security of his sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered his computer to reach the advertised performance. Had Mr. Pollack been aware of these facts, he would not have purchased his processor, or paid substantially less for his processor.

6. Jonathan Caskey-Medina

29. Plaintiff Jonathan Caskey-Medina is a resident and citizen of the State of Massachusetts. On January 6, 2018, Mr. Caskey-Medina purchased a CYBERPOWERPC GUAA2600BS/AMD R5/1TB/8GB/R, containing an AMD Ryzen 5 1400 processor, for $796.86, at the Best Buy in Holyoke, Massachusetts located at 50 Holyoke Street. Mr. Caskey-Medina purchased the computer specifically for gaming and required one with a processor which could handle rendering gaming graphics at the maximum setting. Prior to his purchase, Mr. Caskey-Medina researched different computers on the market to determine the unit that contained the best CPU for his needs.

30. The AMD processor's specifications, including its clock speed or frequency and its reliance on SenseMI Technology, were prominently displayed next to an in-store sample of the computer. Mr. Caskey-Medina reviewed the specification representing that the speed of the processor was 3.2 GHz with a max boost speed of 3.4 GHz and possessed "AMD Sense MI technology" and relied upon that stated speed in making the decision to purchase the computer.

31. Unbeknownst to Caskey-Medina, but known to AMD well before Mr. Caskey-Medina's purchase date, the AMD Ryzen 5 1400 utilized a defective microarchitecture design that allowed an attacker to infiltrate and coerce the processor's caches, as well as its branch prediction and speculative execution processes, to leak data about Mr. Caskey-Medina's most sensitive information. After learning of the Defect in January 2018, Mr. Caskey-Medina installed a "patch"

that purportedly mitigated the risk to his sensitive information presented by the Defect. However, the patch failed to cure the Defect.

32. Moreover, once the patch was applied to Mr. Caskey-Medina's computer, his processor could no longer achieve its advertised performance level, and he was no longer able to run his games at their maximum settings. Once he became aware of the Defect, Mr. Caskey-Medina purchased Norton Security. As a result of the Defect and the performance decrease he experienced, Mr. Caskey-Medina was forced to reduce the graphics settings on his games in order for the games to run at all on his computer.

33. At the time of his purchase, Mr. Caskey-Medina relied on AMD's representations that the AMD processor would perform as advertised and was not defective. Mr. Caskey-Medina was unaware at the time of his purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to his sensitive information; (iii) the AMD CPU that powered his computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of his sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered his computer to reach the advertised performance level. Had Mr. Caskey-Medina been aware of these facts, he would not have purchased his processor, or paid substantially less for his processor.

B. Defendant

34. Defendant AMD is a Delaware corporation with its principal place of business located within this District at 2485 Augustine Drive, Santa Clara, California. AMD was founded in Sunnyvale, California in 1969. Defendant is engaged in the business of designing, manufacturing, selling, and/or distributing CPUs, including the defective processors at issue here. Many of AMD's key executives are based in the District, including AMD's Chief Technology Officer, Mark Papermaster. All references herein to any act of AMD shall include the acts of AMD's directors, officers, employees, affiliates, subsidiaries, and agents where such persons or entities were engaged

in the management, direction, or control of AMD, or where such persons or entities were acting at the direction of AMD.

III. JURISDICTION AND VENUE

35. This Court has general personal jurisdiction over Defendant because it resides within this District.

36. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d) because this matter is a putative class action, the Classes contain members, including Plaintiff, that are citizens of a state different from Defendant, there are more than 100 members of the Classes, and the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000.

37. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because Defendant maintains its principal place of business in this District, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and because Defendant conducts a substantial amount of business in this District.

38. Assignment to the San Jose Division of this District is proper under Northern District of California Civil Local Rule 3-2(c) because a substantial part of the events or omissions which give rise to Plaintiff's claims occurred within the District and Defendant's principal place of business is located in Santa Clara, California. Pursuant to Northern District of California Civil Local Rule 3-2(e), all civil actions which arise in the Santa Clara County shall be assigned to the San Jose Division.

IV. FACTUAL ALLEGATIONS

A. AMD Designed, Manufactured, and Sold CPUs to Plaintiffs and the Classes

39. Founded in 1969, AMD is a leading manufacturer of microprocessors. AMD sells its microprocessors to the marketplace as stand-alone components through third-party retailers. AMD also sells its microprocessors to original equipment manufacturers or OEMs that—with AMD's assistance and guidance—incorporate AMD's microprocessors into, among other things, desktop and laptop computers and servers. OEMs utilizing AMD processors include household names such as Dell Inc., HP Inc., and Lenovo Group Limited.

40. A microprocessor is an integrated electronic circuit that contains all the functions of a CPU of a computer. The CPU is the "brains" of the computing device it powers, responsible for performing all necessary computations for each application and other devices and components connected to the system. Each program communicates with the processor through instructions, with each instruction representing a calculation or operation that the CPU must execute on behalf of the requesting application.

41. When the user asks the computer to perform a function or task, for example, to open a document in Microsoft Word, the CPU: (i) "fetches" the necessary instructions for the task from the computer's memory; (ii) "decodes" the instruction; (iii) "executes" the instruction; and (iv) "writes-back" the result (collectively, the "instruction cycle"). Each step in the instruction cycle takes at least one clock cycle. The number of clock cycles a CPU completes per second is known as the "clock rate." "Clock speed" or "frequency," along with instructions per clock, are ways to measure a CPU's processing speed and is usually expressed in megahertz ("MHz") or gigahertz ("GHz").[1]

42. In 1981, International Business Machines Corp. ("IBM") selected Intel Corp. ("Intel") to supply the CPU for IBM's first personal computer. The processor was known as the Intel 8086. For the 8086, Intel designed an "instruction set," known as x86. The instruction set serves as an interface between a computer's software and hardware. Because IBM allowed OEMs to clone its PC design, IBM PCs and clones thereof soon dominated the market. Each of these computers was powered by a processor that implemented Intel's x86 instruction set. As a result, the x86 instruction set can still be found in virtually every processor designed and manufactured for computers, laptops, and servers, including AMD's CPUs.

43. After the success of the 8086, IBM required Intel to license its next generation processor, the 80286, to a second source supplier, AMD. AMD launched its 80286 clone, the AM286, in 1984. Despite being a clone, the AM286 reached clock speeds nearly 100% greater than Intel's 80286. As a result, Intel refused to provide AMD the right to manufacture clones of its next generation CPU, the 80386, claiming that the second source supplier agreement did not extend

[1] 1,000 MHz equals 1 GHz.

beyond the 80286. AMD was undeterred, designing the AM386 utilizing the x86 instruction set and a reverse-engineered "microarchitecture," which represents the implementation of the CPU's instruction set.

44. Faster and cheaper, the AM386 represented an existential threat to Intel's dominance in the marketplace, leading Intel to file a lawsuit to prevent AMD from releasing it until 1991. Legal entanglements with Intel also impacted the release of the next generation of AMD processors and the last of the Intel clones, the AM486. Ultimately, the parties settled the litigation, leaving AMD with the ability to utilize the x86 instruction set as the basis for its own microarchitecture and CPU design, the first of which was known as K5. Processors based on AMD's K5 microarchitecture debuted in 1995 and relied upon a number of optimization techniques to reach clock speeds of over 100+ MHz.

45. **Instruction Pipelining**. Earlier iterations of AMD's processors utilized "sequential" processing, working through each step of the instruction cycle (e.g., fetch, decode, execute, and write-back) before advancing to the next instruction. The following diagram reflects sequential processing. In this example, it takes eight clock cycles to complete two instructions:

Sequential Processing

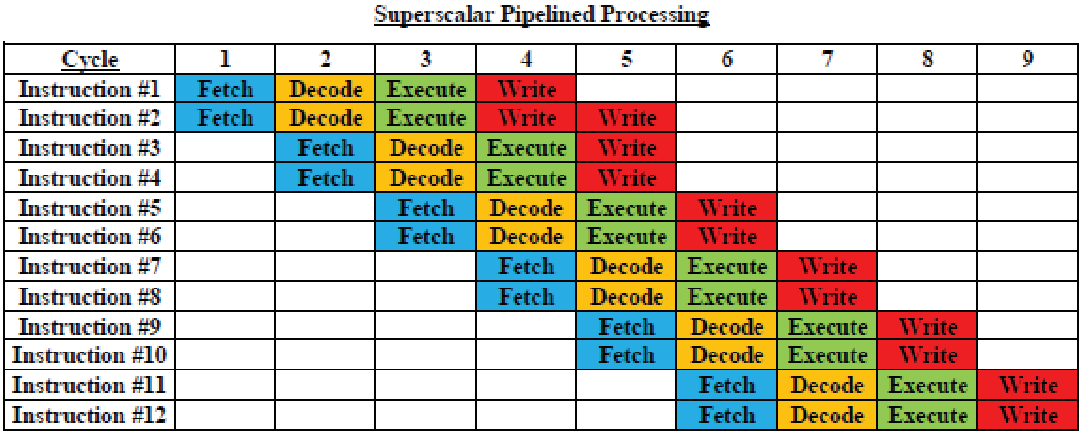
Cycle	1	2	3	4	5	6	7	8	9
Instruction #1	Fetch	Decode	Execute	Write					
Instruction #2					Fetch	Decode	Execute	Write	
Instruction #3									Fetch

46. However, executing instructions in this manner is inefficient. Accordingly, AMD's K5 processors were "pipelined," which allowed the CPU to simultaneously execute multiple instructions. As reflected in the diagram below, a pipelined processor can complete six instruction cycles in nine clock cycles, nearly tripling the work completed in the same amount of time with a sequential processor:

Pipelined Processing

Cycle	1	2	3	4	5	6	7	8	9
Instruction #1	Fetch	Decode	Execute	Write					
Instruction #2		Fetch	Decode	Execute	Write				
Instruction #3			Fetch	Decode	Execute	Write			
Instruction #4				Fetch	Decode	Execute	Write		
Instruction #5					Fetch	Decode	Execute	Write	
Instruction #6						Fetch	Decode	Execute	Write

47. **Superscalar.** AMD's K5 processors also were "superscalar." Whereas pipelining allowed a CPU to process different aspects of multiple instructions at the same time, a superscalar design allowed the CPU to fetch two instructions at the same time, decode two instructions at the same time, and so forth. As reflected in the diagram below, "superscalar" pipelined processors were even more efficient (and therefore faster) than sequential or pipelined processors, completing twelve instructions in nine clock cycles:



Superscalar Pipelined Processing

Cycle	1	2	3	4	5	6	7	8	9
Instruction #1	Fetch	Decode	Execute	Write					
Instruction #2	Fetch	Decode	Execute	Write	Write				
Instruction #3		Fetch	Decode	Execute	Write				
Instruction #4		Fetch	Decode	Execute	Write				
Instruction #5			Fetch	Decode	Execute	Write			
Instruction #6			Fetch	Decode	Execute	Write			
Instruction #7				Fetch	Decode	Execute	Write		
Instruction #8				Fetch	Decode	Execute	Write		
Instruction #9					Fetch	Decode	Execute	Write	
Instruction #10					Fetch	Decode	Execute	Write	
Instruction #11						Fetch	Decode	Execute	Write
Instruction #12						Fetch	Decode	Execute	Write

48. **Out-of-Order Execution**. Superscalar, pipelined processors increase a CPU's capacity to handle multiple instructions at the same time, making it more efficient. However, every application or program has a set of instructions that it wants the CPU to execute in "program order." Instructions can be "data dependent," meaning that the instruction needs the data produced by a preceding instruction in order to execute. Instructions also can be "conditional" expressed as, "if X, then Y." A conditional instruction has to be resolved before the CPU can determine the next step or branch to take. For this reason, such conditional instructions are sometimes called "branch instructions."

49. Data dependent and conditional instructions (among others) can take a number of clock cycles to execute, which causes the superscalar, pipelined CPU to "stall" while it waits for the necessary data or branch it should follow to execute the next instruction. The following diagram shows "program order" or "in order" execution in a superscalar, pipelined processor where Instruction Nos. 1, 3, 5, and 7 take three clock cycles to complete the "execute" stage of the

instruction cycle, leading the CPU to wait to complete Instructions 2, 4, 6, and 8. As a result, the CPU only can complete seven instructions in nine clock cycles:

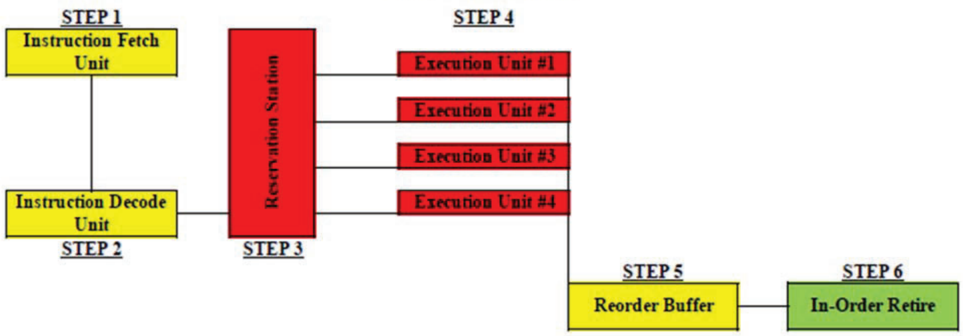
In Order Superscalar Pipelined Processing

Cycle	1	2	3	4	5	6	7	8	9
Instruction #1	Fetch	Decode	Execute			Write			
Instruction #2	Fetch	Decode	Wait			Execute	Write		
Instruction #3		Fetch	Decode	Execute			Write		
Instruction #4		Fetch	Decode	Wait			Execute	Write	
Instruction #5			Fetch	Decode	Execute			Write	
Instruction #6			Fetch	Decode	Wait			Execute	Write
Instruction #7				Fetch	Decode	Execute			Write
Instruction #8				Fetch	Decode	Wait			Execute

50. Engineers developed "out-of-order execution" to make use of the available pipeline resources and clock cycles that might otherwise be wasted. Instead of executing each instruction in "program order," the CPU executes instructions based on "dataflow order," or, in other words, the CPU executes instructions based on an order determined by what data is available to it at any given time. Dataflow order is akin to what students are taught to do with standardized tests—complete questions for which the answer is known first, before going back to those questions for which the answer is not clear.

51. The following diagram shows out-of-order execution. In Steps 1 and 2, the instructions are fetched, decoded, and moved to the Reservation Station. In Step 3, the Reservation Station sends instructions in dataflow order to the Execution Units. During Step 4, the Execution Units execute the instructions and send the results to the Reorder Buffer. Information necessary to execute these instructions is held in the processor's cache. The Reorder Buffer puts the instructions back into "program order" (Step 5) and sends them to be retired in order (Step 6).

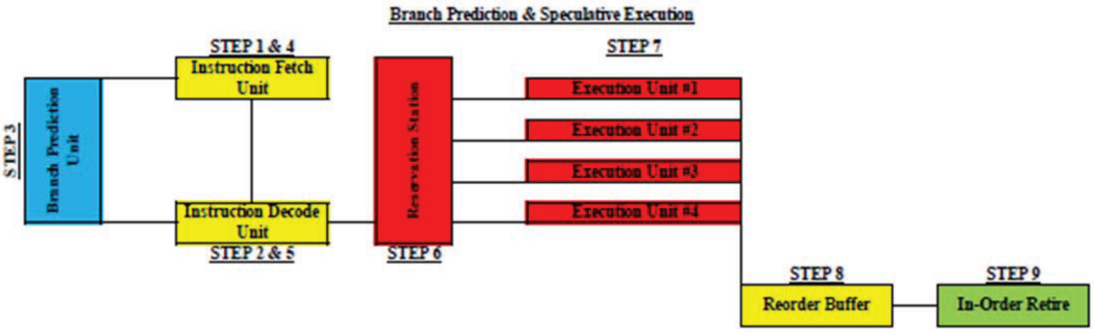
Out-of-Order Execution



52. By relying on out-of-order execution, a CPU can potentially eliminate any idle time associated with waiting for the completion of dependent instructions. AMD's CPUs based on the K5 microarchitecture relied upon out-of-order execution to reach advertised performance levels.

53. **Branch Prediction and Speculative Execution**. While out-of-order execution improves the performance of a superscalar, pipelined CPU by mitigating stalls generated by data dependent instructions, branch prediction and speculative execution address the performance impact associated with conditional instructions. When the CPU fetches and decodes a conditional instruction, the processor predicts the "branch" based on prior results and then speculatively executes instructions down that branch until the conditional instruction is executed and the branch is resolved.

54. The following diagram demonstrates branch prediction and speculative execution. If the CPU fetches and decodes a conditional instruction (Steps 1 and 2), then it will query the Branch Prediction Unit (Step 3) for the branch predictor's "guess" as to which instructions the CPU should fetch next (Step 4). From there, the CPU decodes the instructions based on the branch predictor's guess and speculatively executes the instructions down the predicted path (Steps 5-7).



55. When the CPU eventually executes the conditional instruction, the processor checks whether the branch predictor's guess was correct. If the branch predictor guessed correctly, the processor has performed useful work and the results of the speculatively executed instructions are written to memory (Step 9, above). If the branch predictor guessed incorrectly—a "mis-predicted

branch"—the processor "flushes" its pipeline of the impact of the speculatively executed instructions and proceeds to execute the instructions from the correct path.

56. Beginning with the K5 architecture in 1995, virtually every AMD processor relied upon speculative execution and branch prediction. According to AMD, "[s]peculative execution is a basic principle of all modern processor designs and is critical to supporting high performance hardware."

57. **On-Die Caches**. A computer's memory system holds instructions and data necessary for the CPU to complete its work. When the CPU needs instructions or data to complete a task requested by an application, it must fetch it from the computer's memory. Memory holds all of the instructions and data the CPU utilizes to function. A computer's physical memory space—known as "main memory"—is separated from the CPU on the computer's main circuit board or motherboard.

58. Historically, main memory's frequency or clock speed often was materially slower than the CPU (the "performance gap"). Moreover, the instructions and data stored in memory had to travel to the CPU utilizing a "bus" structure, further extending the time it took to locate and transfer instructions and data to the CPU for processing ("latency"). As a result, while the CPU was able to execute multiple instructions simultaneously, the CPU's capacity was hampered by how fast that information could be obtained from memory. In a 1996 article for the *Microprocessor Report* called, "It's the Memory, Stupid!," a CPU architect presciently noted: "today's [CPUs] are largely able to execute code faster than we can feed them with instructions and data. . . . The real design action is in the memory subsystems – caches, buses, bandwidth, and latency."

59. In order to mitigate the performance gap and the issue of latency, modern CPU microarchitecture design relies on "caches." A "cache" is a location between main memory and the CPU that can be used to temporarily store information and data for use by the CPU. Because caches are typically located on the same "die" (or piece of silicon) as the CPU or in closer proximity to the CPU than main memory on the motherboard, the issue of latency is mitigated. Further, because caches typically operate at the same or similar speed as the CPU, they mitigate the performance gap.

60. Accordingly, AMD's CPUs are designed to first check to see if the instructions or data it needs are in its caches before accessing main memory. If the necessary instructions or data are in its caches (a "cache hit"), the CPU avoids the performance penalty associated with the performance gap and latency. If the necessary instructions or data are not in its caches (a "cache miss"), the CPU simply incurs the performance penalty and accesses main memory. AMD's K5-based CPUs had one on-die cache for instructions and data known as a level 1 or L1 cache and relied upon these caches to reach advertised clock speeds.

B. AMD Advertised Increasingly High CPU Clock Speeds and Performance, Purportedly With the Benefit of Enhanced Security Features

61. For the last 15 years, while AMD has continually touted the advances in its design of caches, branch prediction, and speculative execution, and tied these attributions to increased advertised clock speeds and overall processor performance, it has failed to disclose to consumers that: (i) the CPU's microarchitecture contained the Defect; (ii) the Defect allowed an attacker to gain access to consumers' sensitive information; (iii) AMD CPUs could not reach the advertised speed without relying on defectively designed CPU microarchitecture components that compromised the security of consumers' sensitive information; and (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect.

62. Despite knowing of the Defect that compromised the security of users' most sensitive data, AMD continued to tout the security of its processors. At a basic requirement of any computer, consumers believe that the processor within the computer will adequately protect their sensitive data and that the performance of the processor will not be dependent on exposing their sensitive data. Speaking directly to that reasonable expectation, AMD made public claims about its "[s]trong, hardware-based security" and that it used "[s]tandards-based security features" which "help ensure sensitive data is protected 24/7/365." Such representations, telling consumers what they reasonably expected to hear regarding the security of AMD's processors while simultaneously failing to disclose the existence and scope of the Defect, lulled Plaintiffs and members of the

Classes into the reasonable belief that that AMD's processors would secure their most sensitive information.

1. AMD Failed to Disclose to Consumers that its CPUs Could Not Reach Advertised Performance Specifications Without Compromising the Security of Consumers' Most Sensitive Information

63. The speed at which a CPU performs is a material attribute for consumers purchasing stand-alone AMD CPUs or computers, laptops, and servers powered by AMD processors. Without sufficient processing speed, a CPU will be unable to effectively and efficiently run the device's operating system and software programs, and utilize connected hardware and peripheral devices. To measure a CPU's performance, consumers look to and rely upon the processor's specifications, including, in particular, its clock speed.

64. Since the 1990s, processor manufacturers have placed great emphasis on the clock rate of their processors as an indication of its performance. Beginning with the launch of AMD's first proprietary CPU in 1995, the Company marketed each model of its processors based on its advertised clock speed. AMD's focus on the clock speed of its processors led to the Megahertz Wars, followed by the Gigahertz Wars, during which Intel and AMD battled to see which manufacturer could design a CPU that had the fastest clock speed. The "speed crown" ping-ponged back and forth between the companies, at one point changing hands several times in one quarter in 1999. Both companies claimed to be the first to manufacture and sell a processor with a 1 GHz clock speed in early March 2000.

65. AMD's A10-9600P processor has advertised clock speeds of 2.4 GHz (base) and 3.3 GHz (max boost). AMD's FX 8370 has advertised clock speeds of 4.0 GHz (base) and 4.3 GHz (max boost). AMD's A10-7850K had advertised clock speeds of 3.7 GHz (base) and 4.0 GHz (max boost). AMD's Ryzen R5 1400 processor had advertised clock speeds of 3.2 GHz (base) and 3.4 GHz (max turbo). AMD's website also allows prospective customers to compare the clock speed of each of its processors, and explicitly references its processors' "clocks" as setting its processors apart from the competition. Likewise, websites reviewing and selling AMD processors allow consumers to directly compare the clock speed of available processors.

EXHIBIT 1
Page 21 of 123

66. However, as explained in more detail herein (*see infra* Section IV.C), the design of AMD's CPU microarchitecture created security vulnerabilities that could be easily exploited by attackers, jeopardizing the confidentiality of consumers' sensitive information. While consumers understood that increased CPU efficiency was necessary to achieve advertised speeds, at no point did AMD disclose to consumers the fact that, as designed, their AMD CPUs were susceptible to microarchitectural attacks, the first of which had been identified by no later than 2003.

67. Moreover, consumers were not aware that, despite AMD's knowledge of how to design a secure system (*see infra* Section IV.C.2.a) and the existence of practical microarchitectural attacks (*see infra* Section IV.C.2.b), AMD did nothing to address these vulnerabilities in its CPU microarchitecture design. AMD likewise failed to disclose to consumers that the enhanced performance provided by AMD's CPU exposed their confidential information to practical microarchitectural attacks. Accordingly, consumers purchased AMD CPUs throughout the Class Period unaware that they were sacrificing the security of their sensitive information for increased processing speed.

2. AMD Failed to Disclose to Consumers that its CPUs' Caches Left Consumers' Sensitive Information Exposed

68. By 2003, AMD had hit a wall. Increases in clock speed began to slow. Where the CPU manufacturers were once able to announce materially increased clock speeds every month, now they were lucky to obtain a single digit percentage increase in a single year. One of the primary reasons for this was memory. No longer able to feed a CPU running at aggressive clock speeds with useful instructions, AMD was forced to contend with the speed and capacity of the CPU's memory subsystem in its design of a processor capable of reaching the advertised speeds.

69. A CPU dependent on branch prediction and speculative execution to productively operate at GHz clock speeds, required sufficient cache space in which to buffer necessary instructions and data. To that end, AMD increased the utility of the CPU's cache subsystem in its microarchitecture designs. The number of caches (which store instructions and data within the CPU) increased, from one cache (L1), to two caches (L1 and L2), and finally to three caches (L1, L2, and L3). To address the problem of latency, AMD moved the level 2 ("L2") cache to the CPU

die from its prior location on the motherboard, greatly enhancing the speed of the processors in 1999. In 2003, AMD moved the memory controller from its separate location on the motherboard to the CPU die, which also reduced memory latency.

70. AMD likewise increased the capacity and speed of the on-die CPU caches in its CPU microarchitecture designs. For instance, AMD processors launched in 1995 had a 24 KB L1 cache. One year later, AMD processors had a 64 KB L1 cache. Processors released early in 1999 employing the K6-III architecture boasted two caches, including a 256 KB L2 cache, while processors launched in the latter half of 1999 with the K7 architecture had a 128 KB L1 cache and a 512 KB L2 cache. With the launch of AMD's first dual "core" processors in 2003 (Athlon 64), the K8 architecture boasted two sets of L1 and L2 caches, one for each core, and the L2 cache was now 1 MB. In 2007, AMD added an L3 cache of up to 6 MB that was shared among the cores to its K10 microarchitecture design. Thereafter, the capacity and speed of the caches in AMD's microarchitecture design increased with each iteration in order to ensure that the CPUs could reach advertised performance specifications.

71. The processor's clock speed increased accordingly—whereas processors running the K6-III architecture had advertised max clock speeds of 550 MHz, processors running the K7 (and later, the K75) architecture had advertised max clock speeds of 700 MHz to 2.3 GHz. Processors employing the K10 architecture achieved max clock speeds of 2.6 GHz to 3.7 GHz.

72. However, as explained in more detail herein (*see infra* Section IV.C), the design of AMD's on-die CPU caches created security vulnerabilities that could be easily exploited by attackers, jeopardizing the confidentiality of consumers' sensitive information. While consumers understood that increased CPU efficiency was necessary to achieve advertised speeds, at no point did the Company disclose to consumers the fact that, as designed by AMD, the on-die CPU caches were susceptible to microarchitectural attacks, the first of which had been identified by no later than 2003.

73. Moreover, consumers were not aware that, despite AMD's knowledge of how to design a secure system (*see infra* Section IV.C.2.a) and the existence of practical microarchitectural attacks on the caches within AMD's CPUs (*see infra* Section IV.C.2.b), AMD did nothing to

EXHIBIT 1
Page 23 of 123

address these vulnerabilities in its design of its CPUs' caches. AMD likewise failed to disclose to consumers that the enhanced performance provided by AMD's CPUs due to its memory subsystem design exposed their confidential information to practical microarchitectural attacks. Accordingly, consumers purchased AMD CPUs throughout the Class Period unaware that they were sacrificing the security of their sensitive information for increased processing speed.

3. AMD Failed to Disclose to Consumers That the Design of its Branch Prediction and Speculative Execution Processes Left Consumers' Sensitive Information Exposed

74. To further increase the efficiency, performance, and clock speeds of its CPUs, AMD focused on the CPU's ability to more intelligently utilize branch prediction and speculative execution in its microarchitecture designs. Specifically, AMD identified its "Future Micro-Architectural Innovations," at the October 2003 Microprocessors Forum, including, among other things: (i) "Much higher performance superscalar, out of order CPU core[s];" (ii) "Huge caches;" and (iii) "Branch and memory hints" and enhanced branch predictors.

75. With the launch of its K8 architecture, AMD touted the fact that processors employing K8 had improved accuracy in branch prediction, and the ability to load and store more data necessary to perform "aggressive out of order" execution within the CPU's cache subsystem. This led to material increases in performance, including max clock speeds of up to 3.2 GHz for Athlon 64 X2 processors running K8. As explained in an *ExtremeTech's* April 22, 2003 article, AMD's server offering, the Opteron family of CPUs, had "improved with 'branch selectors' in the L2 cache that reference branch locations in code, and flag the branch types, improve overall efficiency of various branch prediction structures and algorithms" which "contribute[d] to Opteron being able to process more instructions per clock (IPC) than Athlon."

76. In 2006, AMD previewed its "next generation processor technology" at the annual Hot Chips conference, touting its "Balanced, Highly Efficient Cache Structure," including a new L3 cache, and "Improved branch prediction." Thereafter, in 2007, AMD launched its Phenom processors, which utilized the K10 CPU architecture. The K10 architecture contained a number of improvements to further enhance AMD's ability to improve system performance. For instance, the K10 architecture boasted major improvements in the architecture's memory subsystem, to

complement AMD's ability to harness performance efficiencies gained through the use of speculative execution and branch prediction. K10 also had a larger indirect branch predictor and return address stack. Processors employing the K10 architecture achieved max clock speeds of 2.6 GHz to 3.7 GHz.

77. In 2010, AMD announced the launch of two new CPU microarchitecture families—Bulldozer, for mainstream processors, and Bobcat, for low-powered processors. Bulldozer and Bobcat represented a complete redesign of AMD's approach to CPU microarchitecture. In particular, Bulldozer featured "Prediction-Directed Instruction Pre-Fetch," as well as larger pipelines and caches, increasing the processor's ability to fetch and store instructions and data for speculative execution and branch prediction. Processors running the Bulldozer architecture achieved max clock speeds of 4.2 GHz to 4.3 GHz.

78. AMD continued to improve its CPUs' branch prediction and speculative execution processes in follow-on iterations of the Bulldozer microarchitecture family.

79. For instance, AMD launched CPUs based on Steamroller—the third generation of Bulldozer—in early 2014. Steamroller maintained Bulldozer's basic design but included better instruction schedulers, improved branch prediction, and larger and smarter caches. According to an *AnandTech* August 28, 2012 review of Steamroller, while Piledriver—AMD's second generation Bulldozer architecture—boasted a "major design improvement[] . . . in branch prediction," Steamroller "inherit[ed] the perceptron branch predictor from Piledriver, but in an improved form for better performance (mostly in server workloads)."

80. In 2015, AMD launched Excavator, the fourth and final generation of Bulldozer, which included a larger branch target buffer (50% larger as compared to Steamroller-based CPUs), which helped improve performance. When AMD launched the "Carrizo" CPUs based on the Excavator microarchitecture, the Company touted the CPUs' flexibility to invoke multiple processors to execute tasks, which helped preserve laptop battery life, speed up computer applications, and balance the use of PC resources.

81. According to an article published the same day as the "Carrizo" launch, *PCWorld* reported that the Carrizo CPUs capitalized on Excavator's unique engineering which allowed for

EXHIBIT 1
Page 25 of 123

greater performance, including doubling the L1 cache, maintaining latency, and at the same time, cutting the idle power of the CPU from 4.5 to 2.7 watts. *PCWorld* also reported the Excavator cores of the Carrizo CPUs offered 9 to 13 percent more instructions per clock than the prior iterations of Bulldozer microarchitecture, thus providing a performance edge for AMD over rival Intel.

82. However, as explained in more detail herein (*see infra* Section IV.C), the speculative execution and branch prediction processes included in AMD's CPU microarchitecture design created security vulnerabilities that could be easily exploited by attackers, jeopardizing the confidentiality of consumers' sensitive information. While consumers understood that more greater CPU efficiency was necessary to achieve advertised speeds, at no point did AMD disclose to consumers the fact that, as designed by AMD, the branch prediction and speculative execution processes were susceptible to practical microarchitectural attacks, the first of which had been identified by no later than 2006.

83. Moreover, consumers were not aware despite AMD's knowledge of how to design a secure systems (*see infra* Section IV.C.2.a) and the existence of practical microarchitectural attacks on the branch prediction and speculative execution processes within AMD's CPUs (*see infra* Section IV.C.2.b), AMD did nothing to address these vulnerabilities in its design of its CPUs' branch prediction and speculative execution processes. AMD likewise failed to disclose to consumers that the enhanced performance provided by AMD's CPUs due to its branch prediction and speculative execution processes exposed their confidential information to practical microarchitectural attacks. Accordingly, consumers purchased AMD CPUs throughout the Class Period unaware that they were sacrificing the security of their sensitive information for increased processing speed.

4. AMD Failed to Disclose to Consumers That its Much-Vaulted Zen Microarchitecture Left Consumers' Sensitive Information Exposed

84. Ultimately, AMD's Bulldozer architecture had proved disappointing. Despite multiple iterations and improvements upon the basic design to enhance efficiency and performance (*see supra*), AMD CPUs based on this design were not able to fully compete with Intel on the basis of efficiency and performance. Moreover, notwithstanding AMD's efforts to launch competitive

multi-core CPUs, the Company all but lost any meaningful market share in the server market. In response, AMD launched an initiative in 2015 to quickly augment CPU performance in order to gain market share from Intel. According to Kevin Lensing, AMD's Corporate Vice President and General Manager of the Client Business Unit: "Honestly, this was a place we felt like we needed to move fast," Lensing said. "We fell a little back... ***there's a massive focus in the near term to accelerate the pace***."

85. This "massive focus" on CPU performance led to the development of a new CPU microarchitecture family known as "Zen." First announced at an AMD investors meeting in May 2015, the Company designed Zen to offer better CPU performance than other comparable Intel CPUs on the market. At that time, Mark Papermaster, Senior Vice President and Chief Technology Officer for AMD, commented that Zen was "getting right back into the competitive, high-performance CPU. It's a wide open space in terms of bringing competition back to x86." Papermaster also referenced Zen architecture performance upgrades accomplished through a new CPU codenamed "Summit Ridge." Summit Ridge utilized a high-bandwidth caching system that improved internal throughput so memory, cache, and CPUs could communicate faster.

86. These performance upgrades were significant and encompassed a redesign of the cache system to make it more efficient at following instructions. In a March 2016 article on Zen architecture's enhancements, *PCWorld* noted: "AMD has worked on various improvements to boost Zen's CPU performance. AMD has added simultaneous multithreading so virtual machine or highly threaded workloads can be balanced. ***The cache subsystem has been redesigned so tasks can be efficiently fed to execution cores.*** AMD has also removed bottlenecks that hampered earlier architectures, while maintaining power efficiency and performance."

87. Looking back on Zen at the May 2017 Analyst/Investor Day, Papermaster, stated:

> We delivered over 52% of performance gain generationally, and it was really hard-nosed focused engineering effort. It starts with the execution engines. You look at what we did, we widened our execution pipes by 50%. We increased the instruction scheduling by 75%, so you can flow that instruction execution much more effectively each clock tick.
>
> But that only works if you can feed that engine. So what did we do? We have to be able to feed the beast, so we improved on the instruction side with a very smart branch prediction. We actually built in a Perceptron to have much more accuracy,

> a Perceptron engine to give us better accuracy in our branch prediction. We inserted a Micro-Op Cache to more efficiently dispatch those instructions to those pipelines, and then you have to feed it from the data side.
>
> ***We revamped our cache subsystem.*** We increased our cache size. We added a dedicated L3 cache, and we advanced our pre-fetch algorithms, our memory pre-fetch algorithms. Looking at the strides of data, what's the patterns coming in and getting the right data where you need it at the right time.
>
> On top of all of that, we added simultaneous multi-threading. So your execution engines are precious. And so if you do have an install, you're waiting for some data to complete instruction, you want to flip over on a new thread. So simultaneous multi-threading effectively doubles the number of threads. It looks to the operating system like a doubling of the cores available to get any work done.
>
> And what's the result? It's a dramatic improvement of instruction-level parallelism of that execution. Said another way, ***it's a dramatic increase in the performance at every clock tick.*** And so that's what we've done. The team has delivered competitive x86 single-threaded high-performance and hands-down leadership of multi-threaded performance and application development -- and application performance. This achievement absolutely defies industry convention to have this type of gain in a single generational update of CPU design.

88. Since it rolled the Zen microarchitecture out to the market, AMD has manufactured and sold two new lines of processors based on the Zen architecture: the Ryzen family of processors for desktop and laptop computers and EPYC family of processors for servers. In addition to the performance features noted above, all Ryzen processors have SenseMI Technology, which is listed as a "Key Feature" in the specifications for each processor. SenseMI Technology includes "Neural Net Prediction" (predicting the pathway—or branch—that the program will take) which is related to speculative execution functions. According to AMD, "SenseMI technology is a key enabler of AMD's landmark increase of greater than 40 percent in instructions per clock." With EPYC, AMD has successfully re-entered the server market, competing directly with Intel.

89. However, as explained in more detail herein (*see infra* Sections IV.C), the caches and speculative execution and branch prediction processes included in AMD's CPU microarchitecture design, including Zen, created security vulnerabilities that could be easily exploited by attackers, including across Zen-based multi-core and simultaneously threaded CPUs, jeopardizing the confidentiality of consumers' sensitive information. While consumers understood that greater CPU efficiency (including multi-cores and simultaneous threading) was necessary to achieve advertised speeds, at no point did AMD disclose to consumers the fact that, as designed by

AMD, the caches and the branch prediction and speculative execution processes were susceptible to practical microarchitectural attacks, including successful cross-core microarchitectural attacks first demonstrated in 2013.

90. Moreover, consumers were not aware that, despite AMD's knowledge of how to design a secure system (*see infra* Section IV.C.2.a) and the existence of practical microarchitectural attacks on the caches and the branch prediction and speculative execution processes within AMD's CPUs, including cross-core attacks (*see infra* Sections IV.C.2.b-c), AMD did nothing to address these vulnerabilities in its design of these processes. AMD likewise failed to disclose to consumers that the enhanced performance provided by AMD's CPUs due to its caches and branch prediction and speculative execution processes exposed their confidential information to practical microarchitectural attacks, including cross-core attacks. Accordingly, consumers purchased AMD CPUs throughout the Class Period unaware that they were sacrificing the security of their sensitive information for increased processing speed.

5. AMD Failed to Disclose to Consumers That its CPUs Could Not Protect Consumers' Sensitive Information from Exposure to Attackers

91. Beginning with its CPUs based on the Bulldozer microarchitecture, AMD touted the security features of its processors.

92. For instance, in a 2011 marketing document targeted toward public-sector purchasers, AMD identified "Security" as a key component of the "AMD Difference." According to AMD, its Opteron processor-based servers were "setting the new standard for price, performance, and power," and included "[s]trong, hardware-based security . . . that address information-sharing and control at the platform level." AMD further confirmed that it was "ahead of the trends in public sector computing," including "cloud computing," "high performance computing," and "data center consolidation." In an updated version of the same document from 2012, AMD confirmed that it employed "[s]tandards-based security features" which "help ensure sensitive data is protected 24/7/365."

93. AMD likewise noted that it "offer[ed] competitive security features that address[ed] information-sharing at the platform level." AMD also touted the ability of its "virtualized solutions"

EXHIBIT 1

to "improve . . . data security, including AMD-V, which optimized security features to improve performance." Originally code-named "Pacifica" and also known as AMD Secure Virtual Machine (SVM) technology, "AMD-V technology is a set of unique on-chip features that help AMD processor-based clients run multiple operating systems and applications on a single machine by improving the efficiency of virtualization software." Specifically, AMD-V includes "I/O Virtualization," which "[e]nable[d] direct device access by a virtual machine [or "guest" machine], bypassing the hypervisor [or "host" machine] for improved application performance and improved isolation of virtual machines for increased integrity and security."

94. In 2010, AMD launched Vision Pro, a new suite of functionality aimed at businesses. In a 2012 two page marketing circular touting Vision Pro, AMD compared its CPU security offerings with those provided by Intel. Overall, with respect to security, AMD claimed it "has you covered." Specifically, the Company claimed:

> ***AMD's robust silicon-level security features are competitive, consistent, and comprehensive.*** One of AMD's strengths is that security and virtualization technologies are designed into every AMD processor, including our AMD Opteron™ 6000 and 4000 Series processors. Regardless of the unit chosen, customers buying AMD have full access to these features.

95. AMD also confirmed that Advanced Encryption Standard ("AES") instructions, "Processor Virtualization," and "I/O Virtualization" were "important in virtualized environments and in the context of cloud computing." Significantly, all "AMD products beginning with those based on the "Bulldozer" CPU core, including the "Zambezi" desktop processor and the "Interlagos" server processor, have AES instructions."

96. With respect to "Processor Virtualization," AMD confirmed that "Silicon-level," or hardware-based, "virtualization technology allows abstraction of physical system hardware from machine image through the hypervisor, thereby creating a firewall between attackers and physical storage." Further, with respect to "I/O Virtualization," AMD represented that its CPUs "[p]rotect[] memory from peripheral-based attacks, by enabling guest VMs to directly and securely use peripheral devices, such as Ethernet, accelerated graphics cards, and hard-drive controllers." In other words, AMD represented that its CPUs could protect consumers' sensitive information from attacks emanating from other virtual machines and launched through peripheral devices.

97. For embedded solutions (e.g., computers embedded in other devices such as networking hardware), AMD launched DAS 1.0. According to a 2011 marketing document:

> [o]ffering a security solution is especially important for security and regulatory compliance in financial, government, and healthcare applications. However, with many embedded applications, becoming networked and the rise in attacks on these embedded applications, further emphasizes the increasing need for the protection of confidential and sensitive data across a broad range of embedded applications.

98. DAS 1.0 "is a term used to describe the various technologies used to help fulfill the increasing security and reliability needs of embedded solutions. "DAS" included **D**ASH (or Desktop and mobile Architecture for System Hardware), **A**MD-V Technology, and **S**ecurity (or the Trusted Platform Module). AMD claimed that with DAS it was "easy to safeguard systems with comprehensive security from boot-up to shut down with the combination of AMD chip-level security features like TPM support and AMD Virtualization which enable systems to run secure and real-time operating systems in secure, virtualized sessions."

99. Beginning in 2012, AMD partnered with ARM Holdings ("ARM") to develop "secure" CPUs with ARM technology that include ARM "TrustZone®" technology ("TrustZone"). In a June 2012 press release discussing the partnership, AMD Chief Information Officer Mike Wolfe described AMD's partnership with ARM to include "developing a platform security processor using an ARM Cortex(TM)-A5 CPU that features TrustZone technology, to monitor and help protect against malicious access to sensitive data and operations at the hardware level." Shortly after the partnership announcement, *Forbes* reported in a June 18, 2012 article that the partnership goal was to create "a future chip that aligns both AMD x86 and ARM-based hardware to build an ***industry standard security*** solution spanning multiple processor architectures for various devices and operating systems."

100. According to AMD's Senior Technical Writer Lawrence Latif, by December 2015, TrustZone technology had developed to such an extent that it could provide consumers with comfort that their personal data would be protected from "scalable attacks." In fact, in a post entitled "AMD Breakthroughs Server Newsletter – December 2015" he positioned TrustZone as kryptonite to "cyber crime" and "cyber attacks" writing that "ARM TrustZone technology is a

system-wide approach to security, isolating and protecting sensitive applications and interfaces to protect services and devices from scalable attacks. Building on open-standards-based architecture and expanding our collaboration with an extensive network of platform providers, we're working to provide ***the greatest peace of mind on every AMD product***."

101. But contrary to Latif's representations, AMD failed to inform consumers that TrustZone might be susceptible to a cache side-channel attack even though researchers had found it was possible. For example, in an October 2016 article entitled "TruSpy: Cache Side-Channel Information Leakage from the Secure World on ARM Devices" published by the International Association for Cryptologic Research, Virginia Polytechnic Institute and Statue University professors Ning Zhang, Wenjing Lou, and Y. Thomas Hou, professor Kun Sun from George Mason University, and Deborah Shands of the National Science Foundation tested how TrustZone would respond to a mock "TruSpy" side-channel attack into a processor's cache. The professors found Trust Zone had security vulnerabilities to such an attack and warned that "[s]ince our attack relies on one basic design of TrustZone enabled cache architecture and does not use any unique functionalities from a particular version of Android, ***it has impacts on a wide range of ARM processors***."

102. In addition to Zen's increased performance capabilities, AMD offered new security features, also part of the Zen architecture rollout, via the "AMD Secure Processor." The AMD Secure Processor was advertised to consumers as providing secure memory encryption technology ("SME") and secure encryption virtualization technology ("SEV") that was the first of its kind on the market.

103. Beginning in September 2015, AMD touted the AMD Secure Processor as a breakthrough. For example in a blog post AMD Senior Technical Writer Laurence Latif wrote: "the AMD Secure Processor joins other AMD IP innovations from the No Execute Bit to the Secure Asset Management Unit as the future of AMD's security strategy. This type of open-standards innovation has implications across security-dependent use cases, from authentication, geo-fencing, and systems management to remote support, financial transactions, and digital rights management."

104. Industry publications echoed praise for the AMD Secure Processor as a key feature of the Zen architecture. For example, an October 11, 2016 article published by the industry publication WCCFTECH called the AMD Secure Processor's SME the "***holy grail***" because it "allows the complete encryption of the memory being used. Your data is encrypted when it's in transit on the internet….with Zen SME, we can close the last remaining 'cleartext' portion and enable encryption in the memory as well – ***for truly end to end security.***" And the publication, "Tech Power Up," reported on October 12, 2016 that the AMD Secure Processor's SEM and SEV features were an "ace up AMD's sleeve" in competing with rival Intel in the CPU market.

105. However, as explained in more detail herein (*see infra* Sections IV.C), AMD's CPU microarchitecture design created security vulnerabilities that could be easily exploited by attackers, jeopardizing the confidentiality of consumers' sensitive information. While consumers understood that AMD had included features meant to secure consumers' sensitive information from unauthorized access, at no point did AMD disclose to consumers the fact that, as designed by AMD, the caches and the branch prediction and speculative execution processes were susceptible to practical microarchitectural attacks, and none of the security features meant to protect consumers engaging in cloud-based computing could protect against cross-core microarchitectural attacks, including the 2009 attack against an Opteron-powered Amazon server.

106. Moreover, consumers were not aware that AMD did nothing to address these vulnerabilities in its design of these processes, despite AMD's knowledge of how to design a secure system (*see infra* Section IV.C.2.a) and the existence of practical microarchitectural attacks on the caches and the branch prediction and speculative execution processes within AMD's CPUs, including cross-core attacks (*see infra* Sections IV.C.2.b-c). AMD likewise failed to disclose to consumers that the enhanced security features it touted could do nothing to protect consumers' sensitive information from unauthorized access through microarchitectural attacks on the CPUs' caches, and branch prediction and speculative execution processes. Accordingly, consumers purchased AMD CPUs throughout the Class Period unaware that they were sacrificing the security of their sensitive information for increased processing speed.

C. AMD's Processors Are Defective

1. The Defect Explained

107. AMD's use of branch prediction, speculative execution, and caches in its CPU designs has delivered dramatic performance improvements since 1995. However, unbeknownst to Plaintiffs and the Classes, CPUs manufactured and sold by AMD that relied on these processes to achieve advertised performance levels because, as implemented by AMD, these processes created an inherent defect in the CPU that compromised consumers' most sensitive information.

108. "Protecting the confidentiality of secret or sensitive information is a major concern for users of computer systems." Wang, et al "New Cache Designs for Thwarting Software Cache-based Side Channel Attacks" (2007). As such, ensuring the "confidentiality" of secret or sensitive information by preventing its disclosure to a malicious actor is one of the most basic properties of secure computing.

109. One way to protect the confidentiality of sensitive information is by controlling access to it such that only authorized users can read or modify it. Modern CPUs also rely on a number of encryption methods, including the Advanced Encryption Standard ("AES") algorithm, to protect consumers' sensitive information. These protections, however, do not always apply to data about the sensitive information. This is significant. Data about sensitive information can provide powerful clues about the encryption key or the sensitive information itself. For example, how long it takes to access sensitive information can alert an attacker as to whether the sensitive information is present in the CPUs' caches. If an unauthorized person (e.g., an attacker) can gain access to data about sensitive information (e.g., time to access), he can infer the substance of the sensitive information to which he would not otherwise have access, including encryption keys or passwords.

110. Consider the following analogy. An individual (e.g., the attacker) goes to a library (e.g., the computer) to read a book (e.g., data) from a special collection the individual does not have permission to access (e.g., kernel memory). The individual asks the librarian to retrieve "Special Book #1 and the Sue Grafton novel that corresponds to the first letter of page 1 of Special Book #1," (e.g., a program instruction). The librarian retrieves (e.g., fetches) Special Book #1 from the special collection and determines (e.g., decodes) that the first letter on page 1 of that book is "C,"

requiring the librarian to also retrieve "C is for Corpse," by Sue Grafton. The librarian returns to the front desk with Special Book #1 and "C is for Corpse" by Sue Grafton. Before the librarian shows the individual the requested books, she checks his library card. If the individual does not have permission to access books in the special collection, the librarian will put the books on the cart of books to be re-shelved (e.g., the cache) without showing them to the individual.

111. Knowing that the Sue Grafton book with the title corresponding to the first letter on the first page of Special Book #1—the book the individual wants to read but does not have permission to access—is now on the re-shelving cart, the individual begins methodically requesting Sue Grafton books, starting with "A is for Alibi." If the librarian responds, "Please wait while I go and retrieve that book," the individual knows that book is not on the re-shelving cart and the first letter on the first page of Special Book #1 is not A. If, however, the librarian immediately retrieves "C is for Corpse" in response to the individual's request, that action reveals to the individual that the "C is for Corpse" is on the re-shelving cart and, critically, the first letter on page 1 of the Special Book #1 is "C." If it takes nanoseconds to complete these tasks (as it would within a CPU), the individual could determine fairly quickly the contents of Special Book #1 without ever actually seeing the book itself.

112. Accordingly, in order to protect consumers' sensitive information, it is imperative that the CPU is designed to protect from unauthorized access both consumers' sensitive information ***and*** the data about that sensitive information. Despite this, the steps AMD took in its CPU design to address the consequences of "mis-speculation" and the security of its caches were insufficient to protect consumers' sensitive information from unauthorized access.

113. Mis-speculation is a normal function of the CPU when its branch predictor has incorrectly "guessed" the next instructions the CPU needs to execute and the CPU speculatively executes instructions down the mispredicted path. However, both the speculative execution process and the branch predictor in AMD's CPUs can be coerced by an attacker to speculatively execute unnecessary instructions hand-picked by the attacker, leading to intentional mis-speculation. Typically, when mis-speculation occurs, the CPU flushes instructions tied to the mis-speculation

and unrolls the effects of these instructions from its pipeline, but ***does not*** flush its caches of the data used to process these instructions.

114. Neither the CPU nor the computer understands that it is under attack by a malicious actor because mis-speculation is a natural process of the CPU. If the mis-speculation is artificially induced by an exploit, the attacker will be able to control what information is in the cache after the CPU flushes the instructions tied to the artificially induced mis-speculation and unrolls the effects of these instructions from its pipeline. Because the caches within AMD's CPUs are not secure, the attacker can then launch a side-channel attack to leak out data which ultimately leads the attacker to the sensitive information in a manner similar to the library analogy above.

115. Accordingly, AMD's CPU designs allowed an attacker to take advantage of the normal processes of the CPU to obtain data about sensitive information to which the attacker would not otherwise have access. Consumers, including Plaintiffs, purchased these CPUs unaware of this defect or that AMD's CPU design sacrificed the security of consumers' sensitive information to achieve the advertised performance specifications.

2. AMD's Knowledge of the Defect

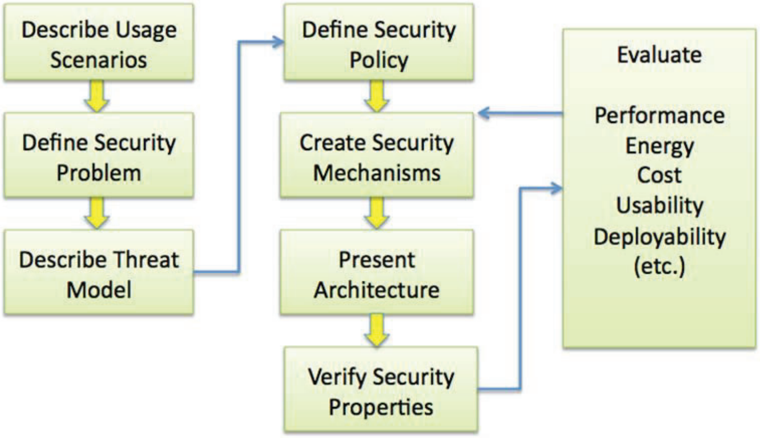
a) AMD Knowledge of Secure System Design

116. In August 2014, then-AMD Corporate Fellow Leendert Van Doorn gave a presentation at an industry conference regarding the design of secure hardware systems. At the time he gave the presentation, Van Doorn was on AMD's leadership team, responsible for AMD's security strategies (including AMD's adoption of the Platform Security Process and other security technologies), and an active participant in AMD's roadmap process, making recommendations regarding hardware to AMD's CEO and senior management.

117. According to Van Doorn, the following were "[c]entral to a secure system design": (i) "[w]ell-defined security properties," e.g., "what are you trying to define, what are your objectives, what are you trying to achieve;" (ii) "threat analysis," e.g., "who is going to be your attacker, how much money are they going to spend on it . . . .;" and (iii) "design methodologies," including "proper test plans, penetration plans, [and] code review." More specifically, he explained that "[y]ou have to very clearly identify who is your attacker, what are you defending against," and

referenced the "Security Architecture Design Methodology," developed and presented by Princeton University's Dr. Ruby Lee.

118. Dr. Lee's methodology, set forth in the diagram below, requires a company like AMD to: (i) describe the relevant computing usage scenarios (e.g., use by a small business); (ii) define "succinctly…the security problem you are trying to solve;" (iii) define the "threat model," or how the threat will present itself to the system including "how much power does the attacker have;" (iv) define a "security policy," or who gets access to what information and when; (v) create "security mechanisms" and incorporate these mechanisms into the CPU's architecture; (vi) "verify" the security properties of the CPU's architecture as a whole; and (vii) evaluate the impact of the security mechanisms on all of the important aspects of CPUs, including performance and cost.



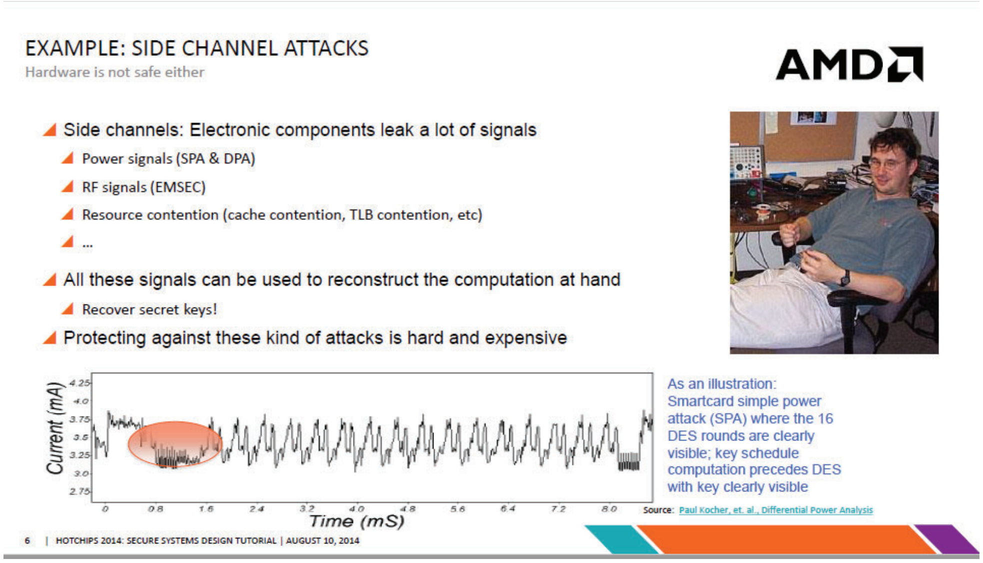
119. According to Lee, for this system to be successful, companies like AMD must "think[] like the attacker" and examine "not just . . . the functionality" of the system "but how would the attacker try to break the system and, if the attacker is breaking the system," how the company can prevent this given its security policies. The goal was not to make the attack "impossible," but to "raise the bar for [the attacker] to successfully attack the system" or, in other words, "to make the attacker's life a lot more difficult" such that the return on his investment is negligible as compared to the cost of mounting the attack in the first instance.

120. That same return on investment, however, was present for companies like AMD in deciding whether and how to address a particular security problem or threat model. As AMD

Corporate Fellow Van Doorn explained during his presentation, designing a secure hardware system was "always a cost/benefit tradeoff," requiring a company to balance "what is the value" of the information "you are protecting," and "the cost that [you] are willing to carry for that," "versus the security you get for that." He noted that while a company should have in place proper test and penetration plans, and code reviews in place, "those kinds of things . . . make the project more costly."

121. To illustrate what happens if you "don't" engage in secure hardware system design, Van Doorn walked through two types of attacks, code injection attacks and side-channel attacks, noting that these are "illustrative of the kind of attacks attackers use." In a side-channel attack, a malicious actor exploits a security vulnerability to access or monitor information about the implementation of a computer system for the purpose of learning about or accessing otherwise privileged information. In this way, private information is deduced from observing the side-effects of operations. Such attacks need not depend on software bugs. Instead, as described here, they rely on the natural function of the hardware and can exploit the vulnerabilities inherent therein.

122. During his presentation, Van Doorn presented the following slide, confirming that it "[p]rotecting against" side-channel attacks "is hard and expensive," noting that side-channel attacks were "***a very, very rich area of attack and a very difficult one to defend against***."



EXAMPLE: SIDE CHANNEL ATTACKS

Hardware is not safe either

- Side channels: Electronic components leak a lot of signals
  - Power signals (SPA & DPA)
  - RF signals (EMSEC)
  - Resource contention (cache contention, TLB contention, etc)
  - ...
- All these signals can be used to reconstruct the computation at hand
  - Recover secret keys!
- Protecting against these kind of attacks is hard and expensive

As an illustration: Smartcard simple power attack (SPA) where the 16 DES rounds are clearly visible; key schedule computation precedes DES with key clearly visible

Source: Paul Kocher, et. al., Differential Power Analysis

6 | HOTCHIPS 2014: SECURE SYSTEMS DESIGN TUTORIAL | AUGUST 10, 2014

123. After Van Doorn raised side-channel attacks during his presentation, Dr. Lee noted:

> ***side-channels [are] really very scary.*** This is correctly executing hardware…that is somehow leaking out your information, like your secret keys. ***This is pretty bad . . .*** and what computer designers must know is [that] ***a lot of your techniques for lowering power or for improving performance make the attacker very happy because it makes his life easy.***"

124. Dr. Lee further concluded: "All current processors with caches are vulnerable – from embedded devices to cloud servers." In fact, according to Lee, "every single piece of hardware that has a cache is vulnerable to cache side channel leakage."

b) AMD's Knowledge of Practical Microarchitectural Attacks

125. Although unknown to the consumer public, the security weaknesses of CPUs reliant on caches, speculative execution, and branch prediction to achieve advertised performance specification was not novel among academics and industry experts, including AMD executives.

126. For instance, since 1995, AMD (but not consumers) has been aware that it was possible to launch an attack to obtain data from a CPU's caches that can be used to infer sensitive information. In a paper titled "The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems," the authors provided their in-depth analysis of Intel's and AMD's pre-1995 CPUs, conducted on behalf of the National Security Agency, concluding that "several features" of these CPUs would "if not properly managed, introduce previously unreported covert channels and other subtle problems." In particular, the authors determined that these "architectural pitfalls" included "covert channels" that "permit one subject (process) to perform an operation that is detectable by another subject, in a way that could violate a system's rules for information flow." Or, in other words, the CPU architecture allowed an unauthorized user to spy upon and learn about sensitive information outside of the typical protections afforded by the kernel/privilege ring set-up described above.

127. The results of the authors' work were "surprising" to them, in that they "did not expect well-defined architectural features to cause undesirable security behavior." However, despite these warnings, AMD increased the number, size, and speed of its on-die caches and incorporated speculative execution and branch prediction into its design for CPUs first launched in 1995 without any safeguards to ensure that an unauthorized user could not "violate a system's rules for

information flow" (e.g., the privilege rings) and learn about consumers' sensitive information stored within the memory of their computer by exploiting the CPU's microarchitecture design.

128. In 2003, two Stanford-based researchers, David Brumley and Dan Boneh, successfully demonstrated a "practical remote timing attack on real applications over a local network" in order "to show that side-channel attacks are a real danger . . . to widely used computer systems." Aciicmez, et al., "Yet Another MicroArchitectural Attack: Exploiting the I-cache" (2006) (citing Brumley, et al., "Remote Timing Attacks are Practical" (2003)). With the publication of Brumley and Boneh's paper, side-channel attacks were no longer a theoretical threat for AMD's consumers. Yet, AMD did not secure its CPUs' caches from these types of attacks.

129. Brumley and Boneh's 2003 discovery led to "increased research efforts on the side-channel analysis of commodity PC platforms" which, in turn, led to the realization "that the functionality of some [CPU] components cause serious side-channel leakage" in 2006. *Id; see also* Wang, et al., "Covert and Side Channels due to Processor Architecture" (2006) ("Information leakage through covert channels and side-channels is becoming a serious problem, especially when these are enhanced by modern processor architecture features."). Researchers began looking critically at "microarchitectural attacks," or attacks that exploit microarchitectural functionalities, like speculative execution, branch prediction, and caches. *Id*.

130. This research demonstrated that microarchitectural attacks were capable of "compromis[ing] the security of computational environments even in the presence of sophisticated protection mechanisms like virtualization and sandboxing." *Id.* For example, in a January 2005 article in *Lecture Notes in Computer Science 2005*, titled "Cache Attacks and Countermeasures: The Case of AES," the authors found that the CPU "cache forms a shared resource which all [of the CPU's] processes compete for, and it thus affects and is affected by every process." These interactions generate metadata. As explained by the authors, "[w]hile the *data* stored in the cache [wa]s protected by virtual memory mechanisms" in the context of this particular exploit, "the *metadata* about the content of the cache, and hence the memory access patterns of [the CPU's] processes using the cache, [wa]s not fully protected" from attack. In the case of AES, this meant

that it was possible to determine the encryption key by observing the metadata stored in the CPU's unsecured cache after the attack.

131. That same year, in an article describing another cache-based microarchitectural attack, or an exploit that "obtain[s] the execution time and/or power consumption of variations generated via cache hits or cache misses," Aciicmez, et al., "Yet Another MicroArchitectural Attack: Exploiting the I-cache" (2006), Daniel Bernstein issued a warning: "I make no claims of novelty for the basic observation that memory-access timings can leak secret information. But these timings are considerably more complicated, considerably easier to exploit, and more difficult to control than indicated in the previous literature on timing attacks." Bernstein, "Cache-timing attacks on AES" (2005).

132. In 2006, researchers identified microarchitectural attacks premised on how speculative execution normally processes exceptions and the natural functionality of the CPU's branch predictor.

133. Specifically, Zhenghong Wang and Dr. Lee found that the normal function of speculative execution in the Intel "Itanium" processor, which allowed the CPU to defer resolving exceptions (e.g., errors that typically arise while a CPU is speculatively executing instructions), could be coerced to speculatively execute instructions to cause a deferred exception, creating a window of time during which the attacker could learn about information he does not have permission to access.

134. Likewise, Onur Aciicmez, Cetin Kaya Koc, and Jean-Pierre Seifert successfully demonstrated two microarchitectural attacks utilizing the CPU's branch predictor. Known as Differential Branch Prediction Analysis and Simple Branch Prediction Analysis, both of these attacks take advantage of the normal process of the CPU's branch predictor and create side-channels to leak information about the CPU's processes to an unauthorized user, similar to the speculative execution attack described by Wang and Lee.

135. Then, in 2007, researchers demonstrated a practical and effective side-channel attack on an instruction cache, taking advantage of its natural function when faced with a "cache conflict." *See* Aciicmez, et al. "Yet Another MicroArchitectural Attack: Exploiting I-cache" (2007). In simple

EXHIBIT 1
Page 41 of 123

terms, a "cache conflict" occurs when there is not enough space in the cache to hold the requisite items for two competing processes. When faced with such a conflict, the cache will evict information it currently is holding. The instruction cache attack uses spy code to create intentional conflicts within the instruction cache, trigging it to evict its contents in favor of the attacker's dummy instructions. Once the instruction cache is filled with the dummy instructions, the attacker allows the CPU to continue with its normal processes for a short period of time, after which the attacker again launches the dummy instructions, measuring how long it takes to execute them, and in so doing, revealing to the attacker the execution flow of the CPU's normal processes.

136. Researchers also pointed to the necessity of conducting "side-channel analysis of computer platforms," given "the recent advances and trends" in the CPU market, "especially the development of microprocessor based security features (e.g. Intel's LT and VT Technologies, AMD Pacifica), and also the recent promises from the Trusted Computing community indicate the security assurance of storing and processing secret values, establishing virtually separate execution environments, etc. on computer platforms." *Id.* For instance, the researchers who identified the instruction cache attack in 2007 also issued a dire warning to the industry regarding the so-called "secure" technologies touted by AMD and Intel:

> The new security and virtualization technologies such as Intel's LT and VT, AMD's Pacifica [aka AMD-V], ARM's Trustzone, software based virtualization mechanisms like those from VMWare are all potentially susceptible to M[icro]A[rchitectural] attacks. We want to emphasize that so far there had not been any publicly known MA attack incidents on these systems. But we believe ***it is only a matter of time until they are shown to be compromised via MA***. ***It is crucial to identify every possible MicroArchitectural vulnerability in order to understand the real potential of MicroArchitectural Analysis and to develop more secure systems by*** employing appropriate software countermeasures and ***making required hardware changes to future architectures***.

137. As a prominent designer and manufacturer of CPUs, AMD was well aware of this research and therefore knew that "the internal functionalities of some microprocessor components like data and instruction cache and branch prediction units cause very serious side-channel leakage and hence create crucial security risks." Aciicmez, et al., "Microarchitectural Attacks and Countermeasures," Cryptographic Measures, Chapter 18 (2008). AMD likewise knew that microarchitectural attacks, including cache-based side-channel attacks, in particular, were

"extremely attractive as a new weapon in the attacker's arsenal" because they are "easy to perform, and are effective on various platforms." Wang, et al., "New Cache Designs for Thwarting Software Cache-based Side Channel Attacks" (2007). AMD also knew that with these types of attacks there is no "need [to] find[] and exploit[] system flaws," because "[t]he [attacker] can achieve his goal [by] "act[ing] like a normal process, performing legitimate operations." *Id.*

138. With clear examples of attackers executing practical attacks that exploited the natural functions of a CPU's speculative execution process (e.g., how it handles exceptions), branch predictor (e.g., its normal analysis process), and caches (e.g., how it handles cache conflicts), AMD was able to define its security objectives and conduct a threat analysis, in order to address the problem of information leakage from its CPU microarchitecture.

139. For example, AMD had the necessary information to explore decreasing the leakage of its CPU microarchitecture or increasing the "noise" of its processes to make it more difficult to isolate information by which an attacker could learn about sensitive information. *See* Haas, "*Side Channel Attacks and Countermeasures for Embedded Systems"*, (Black Hat USA August 2, 2007). It was able to remove "execution time dependence" in the contexts of caches and branch prediction. *Id.* In 2010, Intel was able to develop new instructions for AES ("AES-NI") to partially address the side-channel attacks identified by researchers beginning in 2005. These new instructions ensured that information about AES encryption keys was never stored in the CPU's caches, thereby protecting the keys but not solving the problem posed by cache-based microarchitectural attacks.

140. AMD also possessed the necessary information to take steps to ensure that it had the proper test and penetration plans and code reviews in place to address attacks taking advantage of the natural processes of key elements of a CPU's microarchitecture. For instance, AMD knew how to analogize its CPU microarchitecture to assess its level of vulnerability to side-channel attacks by identifying the potential sources of data leakage, quantifying the leakage rate and comparing to an acceptable or safe margin, and evaluating the effectiveness of countermeasures.

141. In fact, the U.S. government required analyses of susceptibility to side-channel attacks for cryptography modules utilized by the federal government. In July 2007, the National Institute of Standards and Technology ("NIST") issued its first draft of the Federal Information

Processing Standard (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules*, (2007) (Draft), which required the industry to mitigate side-channel attacks in the context of encryption functions, like AES.

142. FIPS 140 is a U.S. Government computer security standard that identifies requirements for four levels of security for cryptographic modules that are utilized by U.S. agencies to protect the security of U.S. information systems. In both the 2007 and 2009 drafts of 140-3, NIST included new requirements to protect against "physical security non-invasive attacks," including "timing analysis attacks." According to a January 2010 presentation by Hirofumi Sakane and Caroline Scace (both of NIST), these "[n]on-invasive attacks [a]re side-channel attacks which exploit weak channels." They "[d]iffer from conventional attacks" because they are "[i]nexpensive" to launch and "leave no tamper evidence" and therefore do not "trigger [a] tamper response."

143. Despite having a clear understanding of the security problem, possible usage scenarios, and the threat model, AMD did not address the security vulnerabilities created by its CPU design.

c) AMD's Knowledge of Cross Core Microarchitectural Attacks

144. The use of the "cloud" to host data and to deploy software and services "introduce[d] a range of new risks," including the "threats from *other customers* due to the subtleties of how physical resources," e.g., CPUs powering servers, "can be transparently shared between *virtual machines* (VMs)." Indeed, as explained in a 2009 article titled, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in order "to maximize efficiency multiple VMs may be simultaneously assigned to execute on the same physical server" and "many cloud providers allow 'multi-tenancy' – multiplexing the virtual machines of disjoint[ed] customers upon the same physical hardware. . . . This in turn, engenders a new threat – that the adversary might penetrate the isolation between VMs (e.g., via vulnerability that allows an 'escape' to the hypervisor or via side-channels *between* VMs) and violated customer confidentiality."

145. More specifically, Thomas Ristenpart, Hovav Shacham, and Stefan Savage of the University of California, San Diego, and Eran Tromer of Massachusetts Institute of Technology warned of the risk of microarchitectural attacks in the cloud environment. Looking at a cloud

environment running on AMD Opteron CPUs, the authors demonstrated that if they could become "a VM co-resident with the target," an attacker might be able to "manipulate shared physical resources (e.g., CPU caches, branch target buffers, network queues, etc.) to learn otherwise confidential information." In other words, cloud computing presented the risk of "cross-VM information leakage due to the sharing of physical resources (e.g., the CPU's data caches)." As such, Ristenpart, et al., "not only demonstrated the grave risks posed by microarchitectural side-channel attacks on user's privacy, but also reignited research in this direction." Irazoqui, et al. "Cross Processor Cache Attacks" (2015).

146. Prior to 2013, an attacker was only able to access information stored in the portions of a CPU or "core" that had access to the shared microarchitectural resource utilized for the attack. This changed with the discovery of a side-channel attack targeting kernel address space layout randomization, or "KALSR," which took advantage of shared resources to deduce information about the location of privileged memory within the kernel, Hund, et al., "Practical Timing Side Channel Attacks Against Kernel Space" ASLR (2013), and the publication of "FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack," the first of multiple papers detailing practical cross-core cache-based side-channel attacks, an attack that is launched from one core to spy on the processes of another core that is "more powerful and hence more dangerous, than prior micro-architectural side-channel attacks."

147. In 2015, researchers identified a number of successful cross-core attacks including, among others: (i) a "prime+probe" attack on an L3 cache, Liu, et al "Last-Level Cache Side-Channel Attacks are Practical," *2015 IEEE Symposium on Security and Privacy* (2015); (ii) a "flush+flush" attack on an L3 cache, Gruss, et al, "Flush+Flush: A Fast and Stealthy Cache Attack" (2015); (iii) a "novel cross-core and cross-VM cache-based side channel attack" on a shared L3 cache, Irazoqui, et al, "S$A: A Shared Cache Attack that Works Across Cores and Defies VM Sandboxing—and its Application to AES" (2015); and (iv) a faster acting, more practical "flush+reload" attack on an L3 cache, Gulmezoglu, et al., "A Faster and More Realistic Flush + Reload Attack on AES" (2015).

148. Significantly, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar, all of Worcester Polytechnic Institute, published a 2015 article titled, “Cross Processor Cache Attacks” which detailed a successful attack against AMD servers with exclusive caches which was capable of “recovering a full AES key . . . within a few seconds.” Known as the “Invalidate + Transfer,” the new attack successfully took advantage of what is known as “cache coherency technologies,” or principles that allow a shared physical resource to manage conflicts between different VMs. Accordingly, as demonstrated by Irazoqui, et al., AMD CPUs were not immune to the new wave of cross-core microarchitectural attacks.

149. Researchers also discovered new microarchitectural vectors for cross-core side-channel attacks. For instance, Sophie D’Antoine, identified a cross-core side-channel attack based on out-of-order execution in her April 2015 master thesis paper, which she ultimately presented at the REcon conference in June 2015 in a presentation titled, “Exploiting Out-of-Order Execution: Processor Side Channels to Enable Cross VM Code Execution.” The presentation confirmed that “physical co-location” with “foreign VMs” led to “side channel vulnerabilities.” Specifically, the allocation of resources between and among VMs and the fact that a VM’s actions are not opaque to other foreign VMs utilizing the same hardware provides a window of opportunity to learn about another VMs information flow and processes, including how the CPU’s microarchitecture scheduled the execution of instructions in order to ensure that CPU maintained peak performance. In this particular attack, D’Antoine remotely triggered the CPU’s typical out-of-order execution process in order to gain access sensitive information of victim VMs, including encryption keys.

150. Researchers likewise discovered that it was possible to launch a cross-core microarchitectural attack from a simple internet browser. In the aptly titled, “The Spy in the Sandbox: Practical Cache Attacks in Javascript and their Implications,” Yossef Oren, Vasileios P. Kemerlis, Simha Sethumadhavan, and Angelos D. Keromytis (all of Columbia University), explained that “to facilitate the attack” which they described “as an extension to the [L3] cache attacks of Liu, et al.,” “the victim needs only to browse to an untrusted webpage that contains attacker-controlled content.” Significantly, the authors were able to map more than 50% of the

EXHIBIT 1
Page 46 of 123

victim's cache in as little as one minute and gain access to the victim's mouse movements and his websites visited.

151. Thereafter, in 2016, Ning Zhang, Wenjing Lou, and Thomas Hou (all of Virginia Polytechnic and State University), Kun Sun of George Mason University, and Deborah Shands of the National Science Foundation published an article entitled, "TruSpy: Cache Side-Channel Information Leakage from the Secure World of ARM Devices." This article identified a new side-channel vector present in ARM's TrustZone technology. As explained above, AMD had relied on TrustZone technology in designing CPUs sold to consumers. TrustZone technology was introduced "to offer security protection via an isolated execution environment called secure world." The design of caches in TrustZone enabled CPUs, including AMD CPUs, "improve[d] system performance," e.g., speed, "by eliminating the need to perform cache flush during world switches." However, by not flushing the cache this design created an exploitable side-channel that allowed the leakage of information from the "secure" environment to the "normal world."

152. Side-channel attacks also were prominently featured in a number of presentations at the August 2016 Black Hat USA conference. In particular, in "Side-Channel Attacks on Everyday Applications," Taylor Hornby (University of Calgary), confirmed that "[s]ide channels affect more than crypto." In "Using Undocumented CPU Behavior to See into Kernel Mode and Break KASLR in the Process," Anders Fogh and Daniel Gruss confirmed that it was possible to take advantage of the normal functionality of the CPU's "pre-fetch" instructions—present in all CPUs utilizing the x86 instruction set—to map kernel memory. The attack Fogh and Gruss described used the hardware's design itself as the "attack vector," and the key takeaways from their research included the fact that "CPU design is security relevant" and "pre-fetch instructions can leak information."

153. Later that same year, in November 2016, Fogh and Michael Schwarz presented "DRAMA: How your DRAM becomes a security problem," another exploit using the hardware design as an attack vector, this time exploiting Dynamic Random Access Memory or DRAM. Similar to the pre-fetch attack, this exploit impacted all CPUs utilizing the x86 instruction set and could be used to "[c]overly extract information across VM, cross CPU," and "[s]py on other

EXHIBIT 1
Page 47 of 123

software," among other things. Once again Fogh had two key takeaways, "DRAM design is security relevant" and "DRAM leaks information."

154. This research provided companies like AMD with a clear understanding of the growing threat of microarchitectural attacks and, in particular, practical side-channel attacks impacting VMs and cloud computing that took advantage of the normal function of a CPU's microarchitecture and could be launched remotely without access to the victim server or computer. AMD also was aware of the consequences of cache designs that failed to flush information in order to avoid hits to performance.

155. It also led the U.S. Government to fund research into secure cache designs. For instance, the U.S. Department of Homeland Security ("DHS") funded researched by Dr. Lee (Princeton University) to design and test a secure cache design. First publicly unveiled in 2007, Dr. Lee's design utilized "moving target defense" to thwart the problem of cache side-channel attacks, which she defined as "[c]orrectly functioning hardware caches [that] leak secret information through cache side-channel attacks," without degrading performance. Typically, if a company wants "high performance you sacrifice security" and if you want "higher security you sacrifice performance." But Dr. Lee's design was a "concrete example" that this trade-off "was not necessary." Commenting on her research during an August 2014 presentation, Dr. Lee noted that it was a "surprising" and "non-intuitive" result but confirmed that this "[t]echnology is ready for industry now" and that DHS "would very much like [the] industry to adopt some of these techniques."

156. Despite being aware of this research, the increased danger of side-channel attacks to VMs and computing in the cloud, and the availability of viable security mechanisms that clearly addressed the side-channel threat without interfering with a CPU's performance, AMD did not address the defect in its CPU design.

d) Plaintiffs Learned AMD Sacrificed The Security of Their Sensitive Information for Speed and Had Sold Them Defective CPUs in January 2018

157. Consumers remained unaware of the defect until January 2018. As an initial matter, because microarchitectural attacks and, in particular, cache side-channel attacks, leave virtually no

trace and are invisible to a computer's OS, these types of attacks cannot be detected by anti-virus software or other mechanisms meant to protect the computer, laptop, or server from malware. Therefore, a consumer utilizing a defective processor would not have any indication that her CPU's microarchitecture is leaking information about the most sensitive data stored within the device.

158. Moreover, ordinary consumers would not have been aware of, have access to, or even have sufficient expertise to understand the ramification of much of the university and industry research. Instead, consumers relied on AMD's representations concerning the security of its CPUs. For instance, certain processors manufactured from 2013 until the present include AMD's platform security process or PSP, known commercially as "AMD Secure Technology." According to AMD's developer's guide for its processors, the PSP is "responsible for creating, monitoring and maintaining the security environment" and "its functions include managing the boot process, initializing various security related mechanisms, and monitoring the system for any suspicious activity or events and implementing an appropriate response."

159. Likewise, with its EPYC processor, AMD sought to reenter the server market with a fast, efficient, and ***secure*** CPU based on the Zen architecture. Commenting on EPYC at the May 2017 Analyst/Investor Day, the SVP and GM of AMD's Enterprise, Embedded, and Semi-Custom Business Group, Forrest Norrod stated:

> And so the way that we're attacking that market is, you guessed it, EPYC. We're attacking that market with a part that Mark and the whole team at AMD has generated, has wrought from those 32 "Zen" cores, offering tremendous power and flexibility. But it's a balanced design. So each "Zen" chip with those 32 cores is coupled to 8 memory channels to keep that beast fed, to keep performance available to applications. We're also adding 128 lanes of high-bandwidth I/O on each EPYC chip, again, so that we can pull in data from the network, from the drives, from flash.
>
> And ***none of this would matter if we didn't also support security***, something that has become all too evident in today's world and we were reminded of earlier this week and over the weekend. ***Security is paramount. Doesn't matter how fast your chip is. If it can't help be part of the security solution, it's part of the problem***. And so that's what we brought.

160. This changed on January 2, 2018 when *The Register* published an article online entitled, "Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign."

The article explained that a design flaw in Intel CPUs necessitated immediate patches to popular operating systems, including Windows, Linux, and macOS.

161. Two days later, *The Register* published another article which explained the defect in clear terms to consumers:

> This is, essentially, a mega-gaffe by the semiconductor industry. As they souped up their CPUs to race them against each other, they left behind one thing in the dust. Security.
>
> One way rival processors differentiate themselves, and perform faster than their competitors is to rely on speculative execution. In order to keep their internal pipelines primed with computer code to obey, they do their best to guess which instructions will be executed next, fetch these from memory, and carry them out. If the CPU guesses wrong, it has to undo the speculatively executed code, and run the actual stuff required.
>
> Unfortunately, the chips in our desktop PCs, laptops, phones, fondleslabs, and backend servers do not completely walk back every step taken when they realize they've gone down the wrong path of code. That means remnants of data . . . remain in their temporary caches, and can be accessed later.

162. Initially, AMD denied that its CPUs contained the Defect, but ultimately confirmed on January 11, 2018 that its CPU design for virtually all AMD processors that utilize the x86 instruction set and rely on speculative execution and branch prediction was defective. As a result, ***all*** of the processors manufactured and sold by AMD since 1995 contain design flaws that allow an attacker to infiltrate and coerce the CPUs' speculative execution and branch prediction processes to force mis-speculation, and subsequently leak through a side-channel metadata regarding consumers' sensitive information from the unsecured caches.

163. After knowing since 2003 that the Defect left consumers' most sensitive information vulnerable to microarchitectural attacks, AMD learned of several new methods pursuant to which attackers could exploit the Defect in June 2017. On May 23, 2018, two additional variants of these exploits were publicly released, one of which was successful in exploiting the defect in AMD CPUs. On July 10, 2018, two more variants were publicly disclosed, one of which was successful in exploiting the defect in AMD CPUs. These attacks have similarities to exploits identified by researchers beginning in 2005 in that these they all involve the attacker artificially inducing a normal function of the CPU's microarchitecture—here, mis-speculation (as compared to, e.g., branch prediction analysis (¶134), exceptions in speculative execution (¶133), and cache conflicts in

the instruction cache (¶135))—and obtained data about sensitive information of the attacker's choosing through a cache-based side-channel attack.

164. Many experts predict that the new wave of microarchitectural attacks exploiting the Defect are just the tip of the iceberg. For instance, Tod Beardsley, research director at Rapid7 (a well-known computer security management and compliance company), noted in a May 22, 2018 *SC Media* article: "Given the complexity and ubiquity of side-channel attacks enabled by speculative execution [(*i.e.,* enabled by the Defect in AMD's CPUs)], I doubt these will be the last variants that will be announced."

D. Attempts to "Patch" the Defect in AMD's CPUs Have Thus Far Inadequate and Materially Impact CPU Performance Once Installed

165. In January 2018, the industry began rolling out patches intended to mitigate the effects of the new wave of microarchitectural exploits first publicly disclosed in January 2018. However, these patches were ad hoc and only defended against certain exploits, if at all; they do not fix the Defect. Some sources, including *Wired* in a January 6, 2018 article, have predicted that the Defect "may be impossible to defend against . . . entirely in the long term without updating hardware." Likewise, as explained by a January 9, 2018 *Scientific American* article, the security vulnerabilities "can only be mitigated—not fixed—at this time" because of the flaw's vast impact to "operating systems, drivers, Web servers and databases."

166. This makes sense. Because the Defect is fully integrated into the design of the CPU's microarchitecture, there is no way to completely eliminate the security vulnerabilities it creates without redesigning the processer. As explained by *Ars Technica* in a January 3, 2018 article:

> while there may be limited ways to block certain kinds of speculative execution, general techniques that will defend against any information leakage due to speculative execution aren't known.
>
> Sensitive pieces of code could be amended to include 'serializing instructions'—instructions that force the processor to wait for all outstanding memory reads and writes to finish (and hence prevent any speculation based on those reads and writes)—that prevent most kinds of speculation from occurring. . . . But these instructions would have to be very carefully placed, with no easy way of identifying the correct placement.

167. Ultimately, AMD has acknowledged that future CPU designs will be needed to support additional security features and that AMD is continuing to evaluate opportunities for new mitigations in both the x86 instruction set and CPU microarchitecture. As such, it is improper to characterize the available "patches" as a "fix." Rather, as Jérôme Boursier, a researcher at Malwarebytes, explained to *Fox News* in January 2018, the patches are simply "a set of workarounds … they aren't a fix. They just change the system behavior to avoid using the bad-designed part of the CPU."

168. Despite the availability of some mitigations for certain, but not all of the attacks that exploit the Defect, AMD has not made a meaningful effort to alert its customers that even the limited mitigations exist. AMD has also not provided any customer support to assist them in implementing the available mitigations. The available mitigations are complicated to implement, even for sophisticated organizations, let alone for individual consumers. As a result, consumers often fail to both access and implement the mitigations that are available.

169. To make matters worse, once consumers utilize these mitigations to "patch" their computers, AMD's CPUs are not able to achieve the advertised performance specifications. As *The Register* explained in a January 2, 2018 article entitled "Kernel-memory-leaking Intel Processor design flaw forces Linux, Windows redesign," discussing the impact of the software "patches":

> It allows normal user programs – from database applications to JavaScript in web browsers – to discern to some extent the layout or contents of protected kernel memory areas.
>
> The fix is to separate the kernel's memory completely from user processes using what's called Kernel Page Table Isolation, or KPTI. . . .
>
> The downside to this separation is that it is relatively expensive, time wise, to keep switching between two separate address spaces for every system call and for every interrupt from the hardware. These context switches do not happen instantly, and they force the processor to dump cached data and reload information from memory. ***This increases the kernel's overhead, and slows down the computer***.

170. *The Register* went on to note that while "[t]he effects are still being benchmarked, . . . we're looking at a ballpark figure of ***five to 30 per cent slow down***, depending on the task and the processor model." According to Mr. Boursier, "[t]hat's because the fix in effect, plugs the vulnerable processes that would otherwise boost performance."

171. Research confirms that software "patches" or updates that have been issued to date have resulted in "corresponding performance slowdowns" given that "the fixes involve routing data for processing in less efficient ways," as explained in a January 6, 2018 *Wired* article. As explained in a November 26, 2018 *Tom's Hardware* article, recent testing has confirmed the performance penalty from mitigation can be up to 50% for Linux users patching just one of the attacks publicly disclosed in January 2018. As such, "when performance goes down by 50% on some loads, people need to start asking themselves whether it was worth it" to use the mitigation.

172. AMD and its partners admit that there is a performance penalty for mitigating the risk of exploitation. Furthermore, Microsoft Corp. has recently acknowledged that patches for computers running Windows operating systems with defective processors result in "a performance impact." Indeed, Microsoft now advises that "[i]n some cases, ***installing these updates will have a performance impact***."

173. The hurried "patches" also have often created problems beyond a performance penalty, such as putting computers into a continuous reboot cycle and in the case of computers powered by AMD CPUs "bricking" them or rendering them inoperable. This has led some manufacturers to recommend that customers stop downloading the patches altogether until the issues can be rectified, leaving consumers in a classic "Catch-22" situation. Even more concerning, some of the patches, including Windows patches, are incompatible with certain, often costly, anti-virus software, preventing some users from receiving the emergency patches at all, or having to disable critical anti-virus software. The patches also have shown to be incompatible with "older" processors, leading AMD to refrain from releasing any patches for its pre-2011 processors that suffer from the Defect. And some publishers report a significant risk of data loss and downtime through patching.

174. Researchers continue to believe that the only long-term fix for the Defect is to totally redesign the CPUs, and there are no new AMD processors on the immediate horizon that are known to definitely solve the Defect without a corresponding diminution of performance.

E. Defendant's Attempts to Limit and Disclaim Warranties are Unconscionable

175. Based on pre-production testing, pre-production design or failure mode analysis, post-production testing and research, much like that done by Google's Project Zero and the Graz University of Technology, and information from third-party researchers given to it in June 2017, Defendant was aware of the defect in its processors but did not correct the defect prior to sale in order to achieve higher processing speeds in their products, which they then falsely marketed as defect-free. This information was not available to Plaintiffs and members of the Classes at the time of their purchases.

176. The average lifespan of a computer is five to six years, but the average lifespan of a computer processor can be longer before there is a failure. As a result, Defendant knew that the defect in the processors would be discovered while most of the processors sold were still in use.

177. Defendant took into account the defect in selecting the durational term of the warranties of two or three years, which was well below the average and expected lifespan of the processors or the computer in which they were installed. Defendant also disclaimed design defects and the implied warranties, because they knew they had designed their processors with the Defect in order to achieve higher processing speeds. These non-negotiable terms were selected unilaterally by Defendant in order to avoid having to honor the warranty for the vast majority of their processors when the defect was inevitably discovered, leaving Plaintiffs and members of the Classes without any warranty protection for the Defect and the damages caused by the Defect.

178. Plaintiffs and members of the Classes lacked the ability to negotiate or even review the terms of the warranty prior to purchase. The warranties are offered on a "take-it-or-leave-it" basis, the terms of which are not available until the product is purchased and the packaging opened. In fact, Defendant published warranty terms on its website, but the terms of the warranty that Plaintiffs received with their products differed from those published. As a result of the difference between the warranty language published by Defendants and the warranty contained in the boxes of the processors or computer purchased by Plaintiffs and members of the Classes, the applicable terms of the warranties were a surprise to Plaintiffs.

179. Plaintiffs and members of the Classes are also without meaningful choice in the selection of processors. Together, AMD and Intel control nearly 100% of the computer processor market. Intel processors are usually more expensive than their AMD counterparts, leaving Plaintiffs and consumers with only one choice for a more affordable processor for their computers: AMD.

180. AMD also disclaims implied warranties, such that AMD provided products to Plaintiffs and the Classes while forcing them to agree that the product would be completely useless, or unfit for its ordinary purpose.

181. There is no reasonable commercial justification for such broad disclaimers and limitations on liability. Defendant had obligations under the Uniform Commercial Code, as well as state and federal law, to not falsely advertise or misrepresent the quality or security of their products, so it cannot be commercially reasonable to attempt to evade those legal obligations by way of disclaimers buried in warranties which are not available for review prior to purchase. Defendant was not selling used products at a yard sale—where an "as is" limitation might be commercially appropriate—it is a technology giant providing a significant portion of the marketplace with the "brains" of their computers.

182. Further, the disclaimers are unenforceable under Cal. Civ. Code § 1668, which prohibits enforcement of contract terms where the contract attempts to "exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent…"

183. Here, to the extent Defendant is seeking to invoke the disclaimers or limitations on liability to avoid responsibility for their violation of several laws, including the CLRA, the UCL, Florida's Deceptive and Unfair Trade Practices Act (" FDUTPA"), Massachusetts General Law Chapter 93A, and Louisiana Civil Code articles 2520 and 2524, among others, they are "against the policy of the law" and cannot be enforced.

V. TOLLING OF THE STATUE OF LIMITATIONS AND ESTOPPEL

184. **Discovery Rule Tolling**. Plaintiffs and members of the Classes could not have reasonably discovered through the exercise of reasonable diligence that their AMD processors

suffered from major security vulnerabilities that, if mitigated, resulted in reduced processing performance, within the time period of any applicable statute of limitations.

185. Plaintiffs and members of the Classes did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendant was concealing a latent defect and/or that the AMD processors contained a defect that exposed them to security vulnerabilities that, if mitigated, resulted in reduced processing performance.

186. **Fraudulent Concealment Tolling**. Throughout the time period relevant to this action, Defendant concealed from and failed to disclose to Plaintiffs and members of the Classes vital information concerning the Defect described herein, despite the fact that Defendant knew the Defect in its Processors well before its discovery by a third party.

187. Defendant kept Plaintiffs and members of the Classes ignorant of vital information essential to the pursuit of their claims. As a result, neither Plaintiffs nor members of the Classes could have discovered the Defect, even upon reasonable exercise of diligence.

188. Despite its knowledge of the Defect, Defendant failed to disclose and concealed, and continues to conceal, critical information relating to the Defect from Plaintiffs and members of the Classes, even though, at any point in time, it could have done so through individual correspondence, media release, or by other means.

189. Plaintiffs and members of the Classes justifiably relied on Defendant to disclose the Defect in the AMD processors they purchased or leased (either directly or as a component of, among other things, a computer or server), because the Defect was hidden and not discoverable through reasonable efforts by Plaintiffs and members of the Classes.

190. Thus, the running of all applicable statutes of limitations have been suspended with respect to any claims that Plaintiffs and members of the Classes have sustained as a result of the defective AMD processors by virtue of the fraudulent concealment doctrine.

191. **Estoppel**. Defendant was under a continuous duty to disclose to Plaintiffs and members of the Classes the true character, quality, and nature of the defective processors and associated security vulnerabilities and reductions in processing performance, but concealed the true nature, quality, and character of the processors.

192. Based on the foregoing, Defendant is estopped from relying on any statutes of limitations in defense of this action.

VI. CLASS ACTION ALLEGATIONS

193. Plaintiffs bring this proposed action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and/or 23(b)(3) on behalf of the following Classes:

> **Nationwide Class**: All persons or entities that purchased or leased one or more AMD processors, or one or more devices containing an AMD processor in the United States within the applicable statute of limitations;
>
> **California Class**: All persons or entities that purchased or leased one or more AMD processors, or one or more devices containing an AMD processor in the state of California within the applicable statute of limitations;
>
> **Florida Class**: All persons or entities that purchased or leased one or more AMD processors, or one or more devices containing an AMD processor in the state of Florida within the applicable statute of limitations;
>
> **Louisiana Class**: All persons or entities that purchased or leased one or more AMD processors, or one or more devices containing an AMD processor in the state of Louisiana within the applicable statute of limitations; and
>
> **Massachusetts Class**: All persons or entities that purchased or leased one or more AMD processors, or one or more devices containing an AMD processor in the Commonwealth of Massachusetts within the applicable statute of limitations.

194. Excluded from the Classes are Defendant and any parents, subsidiaries, corporate affiliates, officers, directors, employees, assigns, successors, the Court, Court staff, Defendant's counsel, and all respective immediate family members of the excluded entities described above. Plaintiff reserves the right to revise the definition of the Classes based upon subsequently discovered information and reserves the right to establish subclasses where appropriate.

195. This action has been brought and may be properly maintained on behalf of the Classes proposed herein under Fed. R. Civ. P. 23.

196. **Numerosity**. Fed. R. Civ. P. 23(a)(1): The Classes are so numerous that individual joinder of all potential members is impracticable. Plaintiffs believe that there are at least thousands of proposed members of the Classes throughout the United States. Members of the Classes may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

197. **Commonality and Predominance**. Fed. R. Civ. P. 23(a)(2) and 23(b)(3): This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Classes, including, without limitation:

A. Whether Defendant engaged in the conduct alleged herein;

B. Whether Defendant's processors are defective;

C. Whether the purported "patches," "fixes," or other remedies are ineffective and/or result in reduced processing performance;

D. Whether any such reduced processing performance is material;

E. Whether Defendant knew that its processors were defective and that, if mitigated, resulted in reduced processing performance;

F. Whether Defendant had a duty to disclose, and breached its duty to disclose, that its processors were defective and that, if mitigated, resulted in reduced processing performance;

G. Whether Defendant intentionally, recklessly, or negligently misrepresented or omitted material facts including the fact that its processors are defective and that, if mitigated, resulted in reduced processing performance;

H. Whether Defendant breached its express warranties in that its processors were defective with respect to manufacture, workmanship, and/or design;

I. Whether Defendant breached its implied warranties in that its processors were defective with respect to manufacture, workmanship, and/or design;

J. Whether Defendant violated the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301, et seq.;

K. Whether Defendant violated California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.;

L. Whether Defendant violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq.;

M. Whether Defendant violated the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, et seq.;

N. Whether Defendant breached its warranty in violation of La. Civ. Code Art 2520, 2524;

O. Whether Defendant committed deceptive acts or practices in violation of Mass. Gen. Laws 93A, §2;

P. Whether Plaintiffs and members of the Classes overpaid for AMD processors;

Q. Whether Defendant made material omissions concerning the true characteristics of the AMD processors, including the existence of significant security vulnerabilities in the processors as designed;

R. Whether members of the Classes would not have purchased or leased—or would have paid significantly less for—AMD processors (or devices containing AMD processors), had Defendant disclosed the Defect;

S. Whether Plaintiffs and members of the Classes are entitled to equitable relief, including, but not limited to, restitution or injunctive relief; and

T. Whether Plaintiffs and members of the Classes are entitled to damages and other monetary relief and, if so, in what amount.

198. **Typicality**. Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of the claims of the other members of the Classes because, among other things, all members of the Classes were comparably injured through Defendant's wrongful conduct as described above.

199. **Adequacy**. Fed. R. Civ. P. 23(a)(4): Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Classes they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously. The interests of the Classes will be fairly and adequately protected by Plaintiffs and their counsel.

200. **Declaratory and Injunctive Relief. Fed. R. Civ. P. 23(b)(2)**: Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Classes, thereby making appropriate final injunctive relief and declaratory relief with respect to the Classes as a whole.

201. **Superiority**. Fed. R. Civ. P. 23(b)(3): A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and members of the Classes are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Classes to individually seek redress for Defendant's wrongful conduct. Even if members of the Classes could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VII. CLAIMS FOR RELIEF

A. California and Nationwide Claims

COUNT I
Violation of California's Consumers Legal Remedies Act ("CLRA")
Cal. Civ. Code § 1750, et seq.
(On Behalf of the Nationwide Class and the California Class)

202. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

203. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

204. Cal. Civ. Code § 1750, *et seq.*, the CLRA, "is to be liberally construed and applied to promote its underlying purposes, which are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection.

205. Plaintiffs and members of the Nationwide and California Classes are "consumers" within the meaning of the CLRA, Cal. Civ. Code § 1761(d).

206. Defendant is a "person" within the meaning of the CLRA, Cal. Civ. Code § 1761(c).

207. AMD's processors are "goods" within the meaning of the CLRA, Cal. Civ. Code § 1761(a).

208. Plaintiffs, the Nationwide Class, and the California Class's purchase or lease of AMD processors, or devices containing AMD processors, are "transactions" within the meaning of the CLRA, Cal. Civ. Code § 1761(e).

209. Defendant violated the CLRA by misrepresenting the performance and security capabilities and features of its processors, and failing to disclose and omitting the existence of the Defect in its processors, because at the time of their purchase, the processors were not both secure ***and*** capable of reaching the advertised speeds as represented by Defendant. As such, Defendant violated the CLRA by:

(a) "[r]epresenting that goods . . . have . . . characteristics, . . . uses, [and] benefits . . . that they do not have…" (Cal. Civ. Code § 1770(a)(5));

(b) "[r]epresenting that goods . . . are of a particular standard, quality, or grade…" (Cal. Civ. Code § 1770(a)(7));

(c) "[a]dvertising goods . . . with intent not to sell them as advertised…" (Cal. Civ. Code § 1770(a)(9)); and

(d) "[r]epresenting that the subject of a transaction has been supplied in accordance with a previous representation when it has not." (Cal. Civ. Code § 1770(a)(16)).

210. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose and omitted the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiffs and members of the Nationwide and California Classes, but failed to do so.

211. Defendant's omissions caused Plaintiffs and members of the Nationwide and California Classes' to be unaware at the time of their purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to their sensitive information; (iii) the AMD CPU that powered their computer could not reach the advertised performance level without relying on

EXHIBIT 1
Page 61 of 123

defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerability created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered their computers to reach the advertised performance level.

212. Defendant's scheme and concealment of the true characteristics of the AMD processors was material to Plaintiffs and the Nationwide and California Classes. The Defect relates to the central functionality of the AMD processors as it affects the processors' ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information. Plaintiffs and the Nationwide Class and the California Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

213. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiffs and the Nationwide and California Classes regarding the security of the processors, Defendant had the duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure and capable of reaching the advertised speeds.

214. Defendant intentionally and knowingly failed to disclose and misrepresented material facts regarding the AMD processors with intent to mislead Plaintiffs and members of the Nationwide and California Classes.

215. Defendant's deceptive conduct was likely to deceive a reasonable consumer, and did in fact deceive reasonable consumers including Plaintiffs and members of the Nationwide and California Classes.

216. Plaintiffs and members of the Nationwide and California Classes reasonably relied upon Defendant's material omissions and misrepresentations. They had no way of knowing that Defendant's representations were false and misleading. Plaintiffs and members of the Nationwide and California Classes did not (and could not) unravel Defendant's deception on their own.

EXHIBIT 1
Page 62 of 123

217. The facts concealed and omitted by Defendant from Plaintiffs and members of the Nationwide and California Classes are material in that a reasonable consumer would have considered them to be important in deciding whether to purchase or lease the AMD processors (or devices containing AMD processors) or pay a lower price. Had Plaintiffs and the Nationwide and California Class members known about the defective nature of AMD processors, they would not have purchased or leased the AMD processors (or devices containing AMD processors), or would not have paid the prices they paid.

218. Defendant's unlawful acts and practices affect the public interest and trade and commerce in the State of California, and present a continuing risk to Plaintiff and members of the Nationwide and California Classes.

219. Defendant's violations of the CLRA were willful and oppressive. Defendant knew that its conduct violated the CLRA.

220. Plaintiffs and members of the Nationwide and California Classes were injured and suffered ascertainable loss, injury-in-fact, and/or actual damage as a proximate result of Defendant's conduct in that respective class members overpaid for their AMD processors and did not receive the benefit of their bargain, and their AMD processors (or devices containing AMD processors) have suffered a diminution in value. These injuries are the direct and natural consequence of Defendant's misrepresentations and omissions.

221. Plaintiffs and members of the Nationwide and California Classes are entitled to, *inter alia*, injunctive relief, costs, attorneys' fees, and other such relief the Court deems appropriate, just, and equitable, in amounts to be determined at trial.

222. With this filing, and on this Count, pursuant to Cal. Civ. Code § 1782(d), Plaintiffs and members of the Nationwide and California Classes seek an order enjoining the above-described unfair and deceptive practices.

223. Plaintiffs and members of the Nationwide and California Classes have provided Defendant with notice of its violations of the CLRA pursuant to Cal. Civ. Code § 1782(a), which is attached hereto as **Exhibit A**. Thirty days having expired and Defendant having failed to provide the requested relief, Plaintiffs seek actual damages under the CLRA.

COUNT II
Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of the Nationwide Class and the California Class)

224. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

225. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

226. Cal. Bus. & Prof. Code § 17200, et seq., the UCL, prohibits "any unlawful, unfair or fraudulent business act or practice."

227. By reason of the conduct alleged herein, Defendant engaged in unlawful business practices within the meaning of the UCL.

228. At all relevant times, Defendant has maintained substantial operations in, regularly conducted business throughout, and engaged in the conduct described herein within the State of California.

229. In the course of its business, Defendant specifically violated the UCL by engaging in the following unlawful business acts and practices:

(a) Violating the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301, et seq.;

(b) Violating the Consumer Legal Remedies Act, Cal. Civ. Code § 1750, et seq.; and

(c) Violating California's False Advertising Law, Cal. Bus. & Prof. Code § 1700, et seq.

230. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiffs and members of the Nationwide and California Classes, but failed to do so. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiffs and the Nationwide and California Classes regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure and capable of reaching the advertised speeds.

EXHIBIT 1
Page 64 of 123

231. Defendant's unlawful business practices were likely to deceive a reasonable consumer. Plaintiffs and members of the Nationwide and California Classes used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

232. Defendant's omissions caused Plaintiffs and members of the Nationwide and California Classes to be unaware at the time of their purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to their sensitive information; (iii) the AMD CPU that powered their computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerability created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered their computers to reach the advertised performance level.

233. Defendant's unlawful business practices and concealment of the true characteristics of the AMD processors were material to Plaintiffs and members of the Nationwide and California Classes. The Defect relates to the central functionality of the AMD processors as it affects the processor's ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information.

234. Defendant misrepresented and failed to disclose the truth with the intention that Plaintiffs and members of the Nationwide and California Classes would rely on the misrepresentations and omissions. Had they known the truth, Plaintiffs and members of the Nationwide and California Classes would not have purchased or leased, or would have paid significantly less for, AMD processors or devices containing AMD processors.

235. As a direct and proximate result of Defendant's misrepresentations and failure to disclose material information, Plaintiffs and members of the Nationwide and California Classes have suffered ascertainable loss and actual damages.

236. The harm caused by this conduct vastly outweighs any legitimate business utility it possibly could have.

237. As a direct and proximate result of Defendant's unlawful business practices, Plaintiffs and members of the Nationwide and California Classes have suffered loss of money.

238. As a result of Defendant's unlawful business practices, Plaintiffs and members of the Nationwide and California Classes are entitled to restitution, including disgorgement of profits, costs, and attorneys' fees in amounts to be determined at trial.

239. Defendant's conduct is or may well be continuing and ongoing. Accordingly, Plaintiffs and members of the Nationwide and California Classes are entitled to injunctive relief to prohibit or correct such ongoing acts of unfair competition, in addition to obtaining equitable monetary relief.

COUNT III
Violation of California's UCL – Unfair Business Practice
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of the Nationwide Class and the California Class)

240. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

241. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

242. Cal. Bus. & Prof. Code § 17200, et seq., the UCL, prohibits "any unlawful, unfair or fraudulent business act or practice."

243. By reason of the conduct alleged herein, Defendant engaged in unfair practices within the meaning of the UCL.

244. At all relevant times, Defendant has maintained substantial operations in, regularly conducted business throughout, and engaged in the conduct described herein within the State of California.

245. In the course of its business, Defendant specifically violated the UCL by engaging in the following unfair business acts and practices:

(a) selling or leasing the AMD processors, either directly or as a component of devices containing such processors, to Plaintiffs and members of the Nationwide and

California Classes, either directly or indirectly through third parties, with knowledge of the Defect in the AMD processors, and failing to disclose that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to Plaintiffs' and members of the Nationwide and California Classes' sensitive information; (iii) the AMD CPU that power their computers could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect; and

(b) marketing the AMD processors as both secure ***and*** of particular processing speeds, and misrepresenting the security and processing speeds of the AMD processors.

246. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described above, greatly outweigh any perceived utility. Indeed, Defendant's failure to disclose the Defect with its processors has no utility, and therefore does not outweigh the harm Plaintiffs suffered as a result of the defective processors.

247. Defendant's actions and omissions were injurious to Plaintiffs and members of the Nationwide and California Classes, directly causing the harms alleged.

248. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See*, e.g., Cal. Bus. & Prof. Code § 17500 (California legislative policy against false advertising); Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them.... The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."). Defendants' acts and omissions, and the injuries caused by them are thus "comparable to or the

same as a violation of the law . . . ." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 187 (1999).

249. Defendant was provided notice of the Defect by independent research teams and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiffs and members of the Nationwide and California Classes, but failed to do so. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiffs and the Nationwide and California Classes regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure and capable of reaching the advertised speeds.

250. Defendant's unfair business practices were likely to deceive a reasonable consumer. Plaintiffs and members of the Nationwide and California Classes used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

251. Defendant's unfair business practices and failure to disclose the true characteristics of the AMD processors were material to Plaintiffs and members of the Nationwide and California Classes. The Defect relates to the central functionality of the AMD processors as it affects the processor's ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information.

252. Defendant misrepresented and failed to disclose the truth with the intention that Plaintiffs and members of the Nationwide and California Classes would rely on the misrepresentations and omissions. Had they known the truth, Plaintiffs and members of the Nationwide and California Classes would not have purchased or leased, or would have paid significantly less for, AMD processors, or devices containing AMD processors.

253. As a direct and proximate result of Defendant's misrepresentations and failure to disclose material information, Plaintiffs and members of the Nationwide and California Classes have suffered ascertainable loss and actual damages.

254. The harm caused by this conduct vastly outweighs any legitimate business utility it possibly could have.

255. Plaintiffs and members of the Nationwide and California Classes are entitled to restitution, including disgorgement of profits, costs, and attorneys' fees in amounts to be determined at trial.

256. Defendant's conduct is or may well be continuing and ongoing. Accordingly, Plaintiffs and members of the Nationwide and California Classes are entitled to injunctive relief to prohibit or correct such ongoing acts of unfair competition, in addition to obtaining equitable monetary relief.

COUNT IV
Violation of California's UCL – Fraudulent Business Practice
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of the Nationwide Class and the California Class)

257. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

258. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

259. Cal. Bus. & Prof. Code § 17200, et seq., the UCL, prohibits "any unlawful, unfair or fraudulent business act or practice."

260. By reason of the conduct alleged herein, Defendant engaged in fraudulent business practices within the meaning of the UCL.

261. At all relevant times, Defendant has maintained substantial operations in, regularly conducted business throughout, and engaged in the conduct described herein within the State of California.

262. In the course of its business, Defendant specifically violated the UCL by engaging in the following fraudulent business acts and practices:

(a) selling or leasing the AMD processors, either directly or as a component of devices containing such processors, to Plaintiffs and members of the Nationwide and California Classes, either directly or indirectly through third parties, with knowledge of the Defect in the AMD processors, and failing to disclose that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to Plaintiffs' and members of the Nationwide and California Classes' sensitive information; (iii) the AMD CPU that power their computers could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect;

(b) omitting the fact in Defendant's public statements, statements to third-party retailers, and on the packaging of its processors that AMD processors were capable of achieving particular speeds only if the data of Plaintiffs and members of the Nationwide and California Classes were made vulnerable to side-channel attacks, with the intent that those statements be relied upon; and/or

(c) knowingly and falsely stating that "there is a near zero risk to AMD processors" following the public exposure of vulnerability to side-channel attacks and only correcting that false statement on January 11, 2018.

263. Defendant's statements regarding the speed and/or security of its processors were objectively verifiable statements of fact, and not mere puffery.

264. The who, what, where, when, and why of Defendant's fraudulent business practices are as follows:

(a) **Who**: Defendant AMD;

(b) **What**: Defendant affirmatively misrepresented and failed to disclose the true security and processing speed of its processors by representing that its processors were both secure ***and*** capable of reaching particular speeds

(c) **Where**: Defendant made its affirmative misrepresentations to Plaintiffs and members of the Nationwide and California Classes on its packaging for its processors, on the packaging by third-party computer and server manufacturers, on in-store displays communicated to retailers by AMD or its authorized manufacturers (e.g., Fry's), and online (e.g., Newegg.com);

(d) **When**: July 6, 2013, September 26, 2014, April 21, 2016, and January 6, 2018; and

(e) **Why**: Because, contrary to AMD's representations and omissions, AMD processors are not secure and are only capable of working at the speed and with the performance as promised at the expense of a significant security vulnerability. Instead, AMD processors are either partially secure ***or*** capable of working at the speed promised.

265. Defendant was provided notice of the Defect by independent research teams no later than June 2017, and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiffs and members of the Nationwide and California Classes, but failed to do so. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiffs and the Nationwide and California Classes regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure ***and*** capable of reaching the advertised speeds.

266. Defendant's fraudulent business practices were likely to deceive a reasonable consumer. Plaintiffs and members of the Nationwide and California Classes used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

267. Defendant's scheme and failure to disclose the true characteristics of the AMD processors were material to Plaintiffs and members of the Nationwide and California Classes as evidenced by, among other things, the massive public outcry once the Defect was disclosed.

Moreover, the Defect relates to the central functionality of the AMD processors as it affects the processor's ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information.

268. Defendant misrepresented and failed to disclose the truth with the intention that Plaintiffs and members of the Nationwide and California Classes would rely on the misrepresentations and omissions. Had they known the truth, Plaintiffs and members of the Nationwide and California Classes would not have purchased or leased, or would have paid significantly less for, AMD processors, or devices containing AMD processors.

269. As a direct and proximate result of Defendant's misrepresentations and failure to disclose material information, Plaintiffs and members of the Nationwide and California Classes have suffered ascertainable loss and actual damages.

270. Plaintiffs and members of the Nationwide and California Classes are entitled to restitution, including disgorgement of profits, costs, and attorneys' fees in amounts to be determined at trial.

271. Defendant's conduct is or may well be continuing and ongoing. Accordingly, Plaintiffs and members of the Nationwide and California Classes are entitled to injunctive relief to prohibit or correct such ongoing acts of unfair competition, in addition to obtaining equitable monetary relief.

COUNT V
Fraud by Omission
(On Behalf of the Nationwide Class and the California Class)

272. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

273. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

274. Defendant intentionally and knowingly omitted material facts about the AMD processors, including the fact the processors have significant security vulnerabilities and that the advertised processer speeds were not available without rendering the processors vulnerable to side-

channel attacks which expose users' private information to potential hacking through such side-channel attacks.

275. Defendant acted with the intent that Plaintiffs and members of the Classes rely on Defendant's omissions so that Defendant could profit from the sale of the processors.

276. Specifically, Defendant's fraudulent omissions include, but are not limited to:

(a) selling or leasing the AMD processors (either directly or as a component of devices containing such processors), to Plaintiffs and members of the Nationwide and California Classes, either directly or indirectly through third parties, with knowledge of the Defect in the AMD processors, and failing to disclose that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to Plaintiffs' and members of the Nationwide and California Classes' sensitive information; (iii) the AMD CPU that power their computers could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect;

(b) omitting the fact in Defendant's public statements, statements to third-party retailers, and on the packaging of its processors that AMD processors were capable of achieving particular speeds only if the data of Plaintiffs and members of the Nationwide and California Classes were made vulnerable to side-channel attacks, with the intent that those statements and omissions be relied upon;

(c) making public statements and statements to third-party retailers regarding the security of AMD processors in tandem with the previously described omissions in order to conceal the Defect and its corresponding security risk from Plaintiffs and members of the Nationwide and California; and/or

(d) failing to disclose that AMD processors were vulnerable to the Defect and only disclosing that fact publicly on January 11, 2018.

277. Defendant's statements and omissions regarding the speed and/or security of its processors were objectively verifiable statements or omissions of fact, and not mere puffery.

278. The who, what, where, and why of Defendant's fraudulent business practices are as follows:

(a) **Who**: Defendant AMD;

(b) **What**: Defendant affirmatively omitted the fact there are significant security vulnerabilities with the processors and that the speed of its processors was only available if consumers' data was left vulnerable by representing that its processors were both secure ***and*** capable of reaching particular speeds;

(c) **Where**: Defendant omitted the existence of the Defect from Plaintiffs and members of the Nationwide and California Classes on its packaging for its processors, on the packaging by third-party computer and server manufacturers, on in-store or online displays communicated to retailers by AMD or its authorized retailers (e.g. Fry's, Newegg.com);

(d) **Why**: Because, contrary to AMD's omissions, AMD processors are not secure and are only capable of working at the speed and with the performance as promised at the expense of a significant security vulnerability. Instead, AMD processors are either partially secure or capable of working at the speed promised.

Defendant was provided notice of the Defect by independent research teams no later than June 2017, and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiffs and members of the Nationwide and California Classes, but failed to do so. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiffs and the Nationwide and California Classes regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure and capable of reaching the advertised speeds.

279. Defendant owed a duty to disclose the Defect in its processors because Defendant possessed superior and exclusive knowledge regarding the defect and the vulnerability to which users' data was exposed. Rather than disclose the defect, Defendant intentionally and knowingly omitted material facts including the existence of the Defect and that the represented processor speeds were only available at the expense of a significant security vulnerability in order to deceive consumers and sell additional processors and avoid the cost of repair or replacement of the defective processors.

280. Defendant's fraudulent acts were likely to deceive a reasonable consumer. Plaintiffs and members of the Nationwide and California Classes used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

281. Defendant's scheme and failure to disclose the true characteristics of the AMD processors were material to Plaintiffs and members of the Nationwide and California Classes, as evidence by, among other things, the massive public outcry once the Defect was disclosed. Moreover, the Defect relates to the central functionality of the AMD processors as it affects the processor's ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information. Defendant knew its omissions were misleading and knew the effect of those omissions.

282. Defendant failed to disclose the truth with the intention that Plaintiffs and members of the Nationwide and California Classes would rely on the omissions. Had they known the truth, Plaintiffs and members of the Nationwide and California Classes would not have purchased or leased, or would have paid significantly less for, AMD processors, or devices containing AMD processors.

283. As a direct and proximate result of Defendant's failure to disclose material information, Plaintiffs and members of the Nationwide and California Classes have suffered actual damages, in an amount to be proven at trial.

COUNT VI
Breach of Express Warranty – Limited Warranty
Cal. Com. Code § 2313
(On Behalf of the Nationwide Class and the California Class)

284. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

285. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

286. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Cal. Com. Code § 2104(1), and a "seller" of the AMD processors under § 2103(1)(d).

287. The AMD processors are and were at all relevant times "goods" within the meaning of Cal. Com. Code § 2105(1).

288. In connection with the purchase of AMD processors sold through the AMD Processor in a Box program, AMD provided a three-year limited warranty for processors sold with a heatsink/fan ("HSF") and a two-year limited warranty for processors sold without an HSF. Both warranties cover defects in the material and workmanship of the AMD processors, and processors that fail to substantially conform to AMD's publicly available specifications.

289. Plaintiffs and members of the Nationwide and California Classes experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant.

290. Plaintiffs and members of the Nationwide and California Classes could not have reasonably discovered the Defect in AMD processors prior to the public disclosure of the Defect by cybersecurity experts, or prior to experiencing a known security hack resulting from the Defect.

291. Defendant breached the express warranty by selling AMD processors that were defective with respect to design, workmanship, and manufacture when Defendant knew its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

292. Because of the existence of the Defect, the AMD processors do not perform as warranted.

293. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

294. Thus, Defendant's two-year and three-year limited warranties fail of their essential purpose and the recovery of Plaintiffs and members of the Nationwide and California Classes is not limited to the remedies of the express limited warranties.

295. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. This reasoning equally applies to any attempt to limit the warranties Defendant furnished directly to Plaintiff and members of the Nationwide and California Classes through its marketing campaign, regardless of whether Plaintiff and members of the Nationwide and California Classes purchased or leased their AMD processors, or devices containing such processors, through the AMD Processor in a Box program.

296. Furthermore, the time limits contained in the express limited warranties Defendant furnished in connection with the AMD Processor in a Box program were also unconscionable and inadequate to protect Plaintiffs and members of the Nationwide and California Classes. Among other things, Plaintiffs and members of the Nationwide and California Classes did not determine these limitations, the terms of which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiffs and members of the Nationwide and California Classes, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

297. Defendant knew that its processors were inherently defective and did not conform to their warranties. Plaintiffs and members of the Nationwide and California Classes were induced into purchasing or leasing AMD processors, or devices containing AMD processors, under false pretenses.

298. Plaintiffs and members of the Nationwide and California Classes have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

299. As a direct and proximate result of Defendant's breach of express warranties, Plaintiffs and members of the Nationwide and California Classes have been damaged in an amount to be determined at trial, including, but not limited to, repair and replacement costs, monetary losses associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT VII
Breach of Express Warranty -- Representations
Cal. Com. Code § 2313
(On Behalf of the Nationwide Class and the California Class)

300. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

301. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

302. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Cal. Com. Code § 2104(1), and a "seller" of the AMD processors under § 2103(1)(d).

303. The AMD processors are and were at all relevant times "goods" within the meaning of Cal. Com. Code § 2105(1).

304. Defendant marketed its processors to Plaintiffs and members of the Nationwide and California Classes, and made affirmative representations, regarding the security ***and*** processing speeds of the processors. These affirmative representations purposefully omitted mention of the Defect or that the speeds of the processors was only possible as a result of the Defect, which left users' sensitive data exposed. At the time of their purchase, ***the processors were not both secure***

EXHIBIT 1

and capable of reaching the advertised speeds, as represented by Defendant. Plaintiffs and members of the Nationwide and California Classes were exposed to, and aware of, these representations.

305. Defendant's express warranties formed the basis of the bargain in Plaintiffs', the Nationwide Class's, and the California Class's decision to purchase or lease AMD processors, or devices containing AMD processors. Defendant's various oral and written representations regarding the AMD processors' security and processing speed constituted express warranties to Plaintiffs and the Nationwide and California Classes.

306. An affirmation of fact, promise, or description made by the seller to the buyer which relates to the goods and becomes a part of the basis of the bargain creates an express warranty that the goods will conform to the affirmation, promise, or description.

307. Plaintiffs and members of the Nationwide and California Classes used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors. As such, Defendant's express warranty regarding the benefits of the AMD processors extends directly to consumers like Plaintiffs and members of the Nationwide and California Classes, who are intended third-party beneficiaries of any contract between Defendant and the retailers where AMD processors, or devices with AMD processors, were sold or leased.

308. Defendant represented that its processors were secure ***and*** of particular processing speeds. AMD processors were not secure—given that they were subject to the Defect–and did not operate at stated processing speeds, given that patches necessary to mitigate the Defect result in reduced processing performance.

309. Plaintiffs and members of the Nationwide and California Classes experienced the existence of the Defect in AMD processors but had no knowledge of the existence of the Defect, which was known and concealed by Defendant.

310. Plaintiffs and members of the Nationwide and California Classes could not have reasonably discovered the Defect in AMD processors prior to the public disclosure of the Defect by cybersecurity experts, or prior to experiencing a known security hack resulting from the Defect.

EXHIBIT 1
Page 79 of 123

311. Because of the existence of the Defect, the AMD processors do not perform as warranted in that they do not both run at the advertised speeds ***and*** compute securely.

312. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

313. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. This reasoning equally applies to any attempt to limit the warranties Defendant furnished directly to Plaintiff and members of the Nationwide and California Classes through its marketing campaign, regardless of whether Plaintiff and members of the Nationwide and California Classes purchased or leased their AMD processors, or devices containing such processors, through the AMD Processor in a Box program.

314. Furthermore, the time limits contained in the express limited warranties Defendant furnished in connection with the AMD Processor in a Box program were also unconscionable and inadequate to protect Plaintiffs and members of the Nationwide and California Classes. Among other things, Plaintiffs and members of the Nationwide and California Classes did not determine these limitations, the terms of which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiffs and members of the Nationwide and California Classes, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

315. Defendant knew that its processors were inherently defective and did not conform to their warranties. Plaintiffs and members of the Nationwide and California Classes were induced

into purchasing or leasing AMD processors, or devices containing AMD processors, under false pretenses.

316. Plaintiffs and members of the Nationwide and California Classes have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

317. As a direct and proximate result of Defendant's breach of express warranties, Plaintiffs and members of the Nationwide and California Classes have been damaged in an amount to be determined at trial, including, but not limited to, repair and replacement costs, monetary losses associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT VIII
Breach of Implied Warranty
Cal. Com. Code §§ 2314 & 2315
(On Behalf of the Nationwide Class and the California Class)

318. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

319. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

320. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Cal. Com. Code § 2104(1), and a "seller" of the AMD processors under § 2103(1)(d).

321. The AMD processors are and were at all relevant times "goods" within the meaning of Cal. Com. Code § 2105(1).

322. A warranty that the AMD processors were in merchantable condition and fit for their ordinary purpose is implied by law pursuant to Cal. Com. Code § 2314.

323. A warranty that the AMD processors were in merchantable condition and fit for their ordinary purpose is implied by law pursuant to Cal. Com. Code § 2314.

324. Defendant knew at the time of sale of the AMD processors that Plaintiffs and members of the Nationwide and California Classes intended to use those processors in an ordinary manner by providing basic security for their sensitive data, and that Plaintiffs and members of the

Nationwide and California Classes were relying on Defendant's skill and judgment to furnish suitable products for this ordinary purpose.

325. Plaintiffs and members of the Nationwide and California Classes purchased or leased AMD processors, or devices containing AMD processors, from Defendant, by and through Defendant's authorized agents for retail sales, or were otherwise expected to be the eventual purchasers or lessors of AMD processors when purchased or leased from a third party. At all relevant times, Defendant was the manufacturer, distributor, warrantor, and/or seller of the relevant processors. Defendant knew of the specific use for which its processors were purchased or leased.

326. AMD processors, when sold or leased and at all times thereafter, were not in merchantable condition and were not fit for their ordinary purpose due to the Defect, and the associated problems and failures caused by the Defect. Thus, Defendant breached its implied warranty of merchantability.

327. Plaintiffs and members of the Nationwide and California Classes used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors. As such, Defendant's implied warranty regarding the benefits of the AMD processors extends directly to consumers like Plaintiffs and members of the Nationwide and California Classes, who are intended third-party beneficiaries of any contract between Defendant and the retailers where AMD processors, or devices with AMD processors, were sold or leased.

328. Defendant marketed its processors to Plaintiffs and members of the Nationwide and California Classes as secure ***and*** of particular processing speeds. Plaintiffs and members of the Nationwide and California Classes were exposed to, and aware of, these representations. Indeed, such representations formed the basis of their respective decisions to purchase or lease AMD processors, or devices containing AMD processors.

329. The AMD processors were defective when they left Defendant's possession because they were not both secure ***and*** capable of achieving their particular, advertised processing speeds and, as such, could not perform according to Defendant's affirmative representations. Therefore,

the AMD processors were not reasonably fit for their intended, anticipated, or reasonably foreseeable use.

330. As a direct and proximate result of Defendant's breach of its implied warranty of merchantability, Plaintiffs and members of the Nationwide and California Classes have been damaged in an amount to be proven at trial.

331. Defendant cannot disclaim its warranties implied by law as it knowingly sold or leased a defective product.

332. Defendant was provided notice of the defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of implied warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

333. Any attempt by Defendant to disclaim or limit the implied warranty of merchantability vis-à-vis Plaintiffs and members of the Nationwide and California Classes is unconscionable and unenforceable. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. Among other things, Plaintiffs and members of the Nationwide and California Classes did not participate in determining any warranty limitations, especially those which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiffs, and members of the Nationwide and California Classes, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

334. Further, as a manufacturer of consumer goods, Defendant is precluded from excluding or modifying an implied warranty of merchantability or limiting customers' remedies for breach of this warranty.

335. Plaintiffs and members of the Nationwide and California Classes have complied with all obligations under the warranty, or otherwise have been excused from performance of said obligations as a result of Defendant's conduct described herein.

336. Defendant's warranties were designed to influence consumers who purchased or leased its processors, including products that contain them.

337. Defendant is estopped by its conduct, as alleged herein, from disclaiming any and all implied warranties with respect to the defective processors.

338. The applicable statute of limitations for the implied warranty claim has been tolled by the discovery rule and Defendant's concealment.

COUNT IX
Violation of the Magnuson-Moss Warranty Act ("MMWA"), 15 U.S.C. § 2301, et seq. (On Behalf of the Nationwide Class and the California Class)

339. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

340. Plaintiffs Elliott, Garcia, and Martinelli (for the purposes of this section, "Plaintiffs") bring this Count on behalf of themselves, the Nationwide Class, and the California Class.

341. Plaintiffs and members of the Nationwide and the California Classes satisfy the MMWA's jurisdictional requirement because this action satisfies the diversity jurisdiction requirements under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

342. Plaintiffs and members of the Nationwide and the California Classes are "consumers" within the meaning of the MMWA, 15 U.S.C. § 2301(3).

343. Defendant is a "supplier" and "warrantor" within the meaning of the MMWA, 15 U.S.C. § 2301(4)-(5).

344. AMD's processors are "consumer products" within the meaning of the MMWA, 15 U.S.C. § 2301(1).

345. The MMWA, 15 U.S.C. § 2310(d)(1), provides a cause of action for any consumer who is damaged by the failure of a warrantor to comply with a written or implied warranties.

346. Defendant provided Plaintiffs and members of the Nationwide and the California Classes with one or more express warranties, which are covered under the MMWA, 15 U.S.C.

§2301(6). In connection with the purchase or lease of AMD processors, or devices containing AMD processors, Defendant directly provided warranty coverage for its processors, or indirectly provided warranty coverage for its processors under one or more manufacturer's warranties.

347. Through written advertisements, Defendant marketed its processors to the Plaintiffs and members of the Nationwide and California Classes as secure ***and*** of particular processing speeds. Indeed, such representations formed the basis of the bargain in Plaintiffs and members of the Nationwide and California Classes' decision to purchase or lease AMD processors, or devices containing AMD processors.

348. Plaintiffs and members of the Nationwide and the California Classes experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant, and have not been provided a suitable repair or replacement of the defective processors free of charge within a reasonable time.

349. Defendant provided Plaintiffs and members of the Nationwide and the California Classes with one or more implied warranties, which are covered under the MMWA, 15 U.S.C. § 2301(7).

350. In connection with the purchase or lease of AMD processors, or devices containing AMD processors, Defendant breached these warranties by misrepresenting the standard, quality, or grade of its processors, and failing to disclose and fraudulently concealing the existence of the Defect in its processors. AMD processors share a common defect in design, workmanship, and manufacture that is prone to security vulnerabilities and fails to operate as represented by Defendant.

351. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors. Under the circumstances, the

remedies available under any informal settlement procedure would be inadequate and any requirement that Plaintiffs and members of the Nationwide and the California Classes resort to an informal dispute resolution procedure and/or afford Defendant a reasonable opportunity to cure their breach of warranties is excused and thereby deemed satisfied.

352. Any attempt by Defendant to disclaim or limit its express or implied warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. Among other things, Plaintiffs and members of the Nationwide and California Classes did not participate in determining any warranty limitations, especially those which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiffs and members of the Nationwide and the California Classes, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

353. Plaintiffs and members of the Nationwide and the California Classes would suffer economic hardship if they returned their AMD processors, or devices containing the AMD processors, but did not receive the return of all payments made by them to Defendant. Thus, Plaintiffs and members of the Nationwide and the California Classes have not reaccepted their AMD processors by retaining them.

354. The amount in controversy of Plaintiffs and members of the Nationwide and the California Classes' individual claims meets or exceeds the sum of $25. The amount in controversy of this action exceeds the sum of $50,000, exclusive of interest and costs, computed on the basis of all claims to be determined in this lawsuit.

355. Plaintiffs and members of the Nationwide and the California Classes, individually and on behalf of the respective Classes, seek all damages permitted by law, including diminution in the value of the AMD processors, in an amount to be proven at trial.

COUNT X
Negligence
(On Behalf of the Nationwide Class and the California Class.)

356. Plaintiffs no longer assert a negligence claim.

B. Florida Counts

COUNT XI
Violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA")
Fla. Stat. § 501.201, et seq.
(On Behalf of the Florida Class)

357. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

358. This Count is brought on behalf of Plaintiff Pollack (for the purposes of this section, "Plaintiff") and the Florida Class.

359. The stated purpose of the FDUTPA is to "protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

360. Plaintiff and Florida Class members are each "consumers," and Defendant is engaged in "trade or commerce" within the meaning of the statute. Fla. Stat. § 501.203(7)-(8).

361. FDUTPA declares unlawful "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

362. In the course of its business, Defendant violated FDUTPA by misrepresenting the performance, security capabilities, and features of its processors, and failing to disclose and fraudulently concealing the existence of the Defect in its processors. Specifically, in marketing, offering for sale, and selling the AMD processors, Defendant engaged in one or more of the following unfair or deceptive acts or practices prohibited by Fla. Stat. § 501.204(1):

(a) representing that the AMD processors have characteristics or benefits that they do not have;

(b) representing that the AMD processors are of a particular standard and quality when they are not;

(c) advertising the AMD processors with the intent not to sell them as advertised;

(d) engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or

(e) using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon such concealment, suppression, or omission, in connection with the advertisement and sale of the AMD processors.

363. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose and fraudulently concealed the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiff and members of the Florida Class, but failed to do so.

364. Defendant's omissions caused Plaintiff and members of the Florida Class to be unaware at the time of their purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to their sensitive information; (iii) the AMD CPU that powered their computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerability created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered their computers to reach the advertised performance level.

365. Defendant's scheme and concealment of the true characteristics of the AMD processors was material to Plaintiff and the Florida Class, and Defendant misrepresented, concealed, or failed to disclose the truth with the intention that Plaintiff and the Florida Class would rely on the misrepresentations, concealments, and omissions. Had Plaintiff and the Florida Class members known about the defective nature of AMD processors, they would not have purchased or leased the AMD processors, or devices containing AMD processors, or would have paid significantly less for them.

EXHIBIT 1

366. Plaintiff and the Florida Class members had no way of discerning that Defendant's representations that its processers were both secure ***and*** of a particular processing speed were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose.

367. Defendant had an ongoing duty to Plaintiff and the Florida Class to refrain from unfair and deceptive practices under FDUTPA in the course of its business. Specifically, Defendant owed Plaintiff and the Florida Class members a duty to disclose all the material facts concerning the AMD processors because it intentionally concealed such material facts from Plaintiff and the Florida Class, and/or it made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

368. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiffs and the Nationwide and California Classes regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure ***and*** capable of reaching the advertised speeds.

369. Defendant's deceptive conduct was likely to deceive a reasonable consumer and did in fact deceive reasonable consumers including Plaintiff and members of the Florida Class.

370. Plaintiff and the Florida Class members were injured and suffered ascertainable loss and actual damage as a direct and proximate result of Defendant's conduct in that respective class members overpaid for their AMD processors (or devices containing AMD processors) and did not receive the benefit of their bargain, and their AMD processors (or devices containing AMD processors) have suffered a diminution in value. These injuries are the direct and natural consequence of Defendant's concealment, misrepresentations and/or omissions.

371. Pursuant to Fla. Stat. § 501.211(1), Plaintiff and Florida Class members seek a declaratory judgment and Court Order enjoining Defendant's above-described wrongful acts and practices, and for damages, restitution, and disgorgement. Additionally, pursuant to Fla. Stat. §§ 501.211(2) and 501.2105, Plaintiff and the Florida Class asserts claims for damages, attorney fees, and costs.

EXHIBIT 1
Page 89 of 123

COUNT XII
Fraud by Omission
(On Behalf of the Florida Class)

372. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

373. This Count is brought on behalf of Plaintiff Pollack (for the purposes of this section, "Plaintiff") and the Florida Class.

374. Defendant intentionally and knowingly omitted material facts about its AMD processors, including the fact that the processors have significant security vulnerabilities and that the advertised processer speeds were not available without rendering the processors vulnerable to potential hacking through side-channel attacks, which expose users' private information..

375. Defendant acted with the intent that Plaintiff and members of the Florida Class rely on Defendant's omissions so that Defendant could profit from the sale of the processors.

376. Specifically, Defendant's fraudulent omissions include, but are not limited to:

(a) selling or leasing the AMD processors (either directly or as a component of devices containing such processors), to Plaintiff and members of the Florida Class, either directly or indirectly through third parties, with knowledge of the Defect in the AMD processors, and failing to disclose that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to Plaintiff's and members of the Florida Class' sensitive information; (iii) the AMD CPU that power their computers could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect;;

(b) omitting the fact in Defendant's public statements, statements to third-party retailers, and on the packaging of its processors that AMD processors were capable of achieving particular speeds only if the data of Plaintiffs and members of the Florida Class were made vulnerable to side-channel attacks, with the intent that those statements and omissions be relied upon;

EXHIBIT 1
Page 90 of 123

(c) making public statements and statements to third-party retailers regarding the security of AMD processors in tandem with the previously described omissions in order to conceal the Defect and its corresponding security risk from Plaintiff and members of the Florida Class; and/or

(d) failing to disclose that AMD processors were vulnerable to the Defect and only disclosing that fact publicly on January 11, 2018.

377. Defendant's statements and omissions regarding the speed and/or security of its processors were objectively verifiable statements or omissions of fact, and not mere puffery.

378. The who, what, where, and why of Defendant's fraudulent business practices are as follows:

(a) **Who**: Defendant AMD;

(b) **What**: Defendant affirmatively omitted the fact there are significant security vulnerabilities with the processors and that the speed of its processors was only available if consumers' data was left vulnerable by representing that its processors were both secure and capable of reaching particular speeds;

(c) **Where**: Defendant omitted the existence of the Defect from Plaintiffs and members of the Florida Class on its packaging for its processors, on the packaging by third-party computer and server manufacturers, on in-store or online displays communicated to retailers by AMD or its authorized retailers (e.g. Fry's, Newegg.com); and/or

(d) **Why**: Because, contrary to AMD's omissions, AMD processors are not secure and are only capable of working at the speed and with the performance as promised at the expense of a significant security vulnerability. Instead, AMD processors are either partially secure or capable of working at the speed promised.

379. Defendant was provided notice of the Defect by independent research teams no later than June 2017, and knew of the existence of the Defect much earlier. Nevertheless, Defendant failed to disclose the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiff and members of the Florida Class, but

failed to do so. Defendant had a duty to disclose that the AMD processors were defective because, having volunteered to provide information to Plaintiff and the Florida Class regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure ***and*** capable of reaching the advertised speeds.

380. Defendant owed a duty to disclose the Defect in its processors because Defendant did not disclose that the advertised speeds for AMD processors were only available at the expense of a significant security vulnerability, which constitutes a partial disclosure. Rather than disclose the defect, Defendant intentionally and knowingly omitted materials facts, including the existence of the Defect and that the represented processor speeds were only available at the expense of a significant security vulnerability in order to deceive consumers and sell additional processors and avoid the cost of repair or replacement of the defective processors.

381. Defendant's fraudulent acts were likely to deceive a reasonable consumer. Plaintiff and members of the Florida Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

382. Defendant's scheme and failure to disclose the true characteristics of the AMD processors were material to Plaintiff and members of the Florida Class, as evidence by, among other things, the massive public outcry once the Defect was disclosed. Moreover, the Defect relates to the central functionality of the AMD processors as it affects the processor's ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information. Defendant knew its omissions were misleading and knew the effect of those omissions.

383. Defendant failed to disclose the truth with the intention that Plaintiff and members of the Florida Class would rely on the omissions. Had they known the truth, Plaintiff and members of the Florida Class would not have purchased or leased, or would have paid significantly less for, AMD processors or devices containing AMD processors.

EXHIBIT 1
Page 92 of 123

384. As a direct and proximate result of Defendant's failure to disclose material information, Plaintiff and members of the Florida Class have suffered actual damages, in an amount to be proven at trial.

COUNT XIII
Breach of Express Warranty – Limited Warranty
Fla. Stat. § 672.313
(On Behalf of the Florida Class)

385. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

386. This Count is brought on behalf of Plaintiff Pollack (for the purposes of this section, "Plaintiff") and the Florida Class.

387. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Fla. Stat. § 672.104(1), and a "seller" of the AMD processors under § 672.103(1)(d).

388. The AMD processors are and were at all relevant times "goods" within the meaning of Fla. Stat. § 672.105(1).

389. In connection with the purchase of AMD processors sold through the AMD Processor in a Box program, AMD provided a three-year limited warranty for processors sold with a heatsink/fan ("HSF") and a two-year limited warranty for processors sold without an HSF. Both warranties cover defects in the material and workmanship of the AMD processors, and processors that fail to substantially conform to AMD's publicly available specifications.

390. Plaintiff and members of the Florida Class experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant.

391. Plaintiff and the Florida Class could not have reasonably discovered the Defect in AMD processors prior to the public disclosure of the Defect by cybersecurity experts or prior to experiencing a known security hack resulting from the Defect.

392. Defendant breached the express warranty by selling AMD processors that were defective with respect to design, workmanship, and manufacture when Defendant knew its

processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

393. Because of the existence of the Defect, the AMD processors do not perform as warranted.

394. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

395. Thus, Defendant's two-year and three-year limited warranties fail of their essential purpose and the recovery of Plaintiff and members of the Florida Class is not limited to the remedies of the express limited warranties.

396. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. This reasoning equally applies to any attempt to limit the warranties Defendant furnished directly to Plaintiff and members of the Florida Class through its marketing campaign, regardless of whether Plaintiff and members of the Classes purchased or leased their AMD processors, or devices containing such processors, through the AMD processor in a Box program.

397. Furthermore, the time limits contained in the express limited warranties Defendant furnished in connection with the AMD processor in a Box program were also unconscionable and inadequate to protect Plaintiff and members of the Florida Class. Among other things, Plaintiff and members of the Florida Class did not determine these limitations, the terms of which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Florida Class, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its

processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

398. Defendant knew that its processors were inherently defective and did not conform to their warranties. Plaintiff and members of the Florida Class were induced into purchasing or leasing AMD processors, or devices containing AMD processors, under false pretenses.

399. Plaintiff and members of the Florida Class have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

400. Accordingly, Plaintiff and the Florida Class assert as remedies all actual, incidental, and consequential damages as allowed.

401. As a direct and proximate result of Defendant's breach of its express warranty, Plaintiff and the Florida Class members have been damaged in an amount to be determined at trial, including, but not limited to, repair and replacement costs, monetary losses associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT XIV
Breach of Express Warranty -- Representations
Fla. Stat. §672.313
(On Behalf of the Florida Class)

402. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

403. This Count is brought on behalf of Plaintiff Pollack (for the purposes of this section, "Plaintiff") and the Florida Class.

404. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Fla. Stat. § 672.104(1), and a "seller" of the AMD processors under § 672.103(1)(d).

405. The AMD processors are and were at all relevant times "goods" within the meaning of Fla. Stat. § 672.105(1).

406. Defendant marketed its processors to Plaintiff and the members of the Florida Class, and made affirmative representations, as to the security ***and*** processing speeds of the processors. These affirmative representations purposefully omitted mention of the Defect or that the speeds of

EXHIBIT 1
Page 95 of 123

the processors were only possible as a result of the Defect, which left users' sensitive data exposed. At the time of their purchase, ***the processors were not both secure and capable of reaching the advertised speeds, as represented by Defendant***. Plaintiff and the members of the Florida Class were exposed to, and aware of, these representations.

407. Defendant's express warranties formed the basis of the bargain in Plaintiff and the Florida Class's decision to purchase or lease AMD processors, or devices containing such AMD processors. Defendant's various oral and written representations regarding the AMD processors' security and processing speed constituted express warranties to Plaintiff and the Florida Class.

408. An affirmation of fact, promise, or description made by the seller to the buyer which relates to the goods and becomes a part of the basis of the bargain creates an express warranty that the goods will conform to the affirmation, promise, or description.

409. Defendant represented that its processors were secure and of particular processing speeds. AMD processors were not secure—given that they were subject to the Defect—and did not operate at stated processing speeds, given that patches necessary to mitigate the Defect result in reduced processing performance.

410. Plaintiff and members of the Florida Class experienced the existence of the Defect in AMD processors but had no knowledge of the existence of the Defect, which was known and concealed by Defendant.

411. Plaintiff and the Florida Class could not have reasonably discovered the Defect in AMD processors prior to the public disclosure of the Defect by cybersecurity experts or prior to experiencing a known security hack resulting from the Defect.

412. Because of the existence of the Defect, the AMD processors do not perform as warranted.

413. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and, on information and belief, has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the

Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

414. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. This reasoning equally applies to any attempt to limit the warranties Defendant furnished directly to Plaintiff and members of the Florida Class through its marketing campaign, regardless of whether Plaintiff and members of the Classes purchased or leased their AMD processors, or devices containing such processors, through the AMD Processor in a Box program.

415. Furthermore, the time limits contained in the express limited warranties Defendant furnished in connection with the AMD Processor in a Box program were also unconscionable and inadequate to protect Plaintiff and members of the Florida Class. Among other things, Plaintiff and members of the Florida Class did not determine these limitations, the terms of which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Florida Class, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

416. Defendant knew that its processors were inherently defective and did not conform to their warranties. Plaintiff and members of the Florida Class were induced into purchasing or leasing AMD processors, or devices containing AMD processors, under false pretenses.

417. Plaintiff and members of the Florida Class have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

418. Accordingly, Plaintiff and the Florida Class assert as remedies all actual, incidental, and consequential damages as allowed. As a direct and proximate result of Defendant's breach of its express warranty, Plaintiff and the Florida Class members have been damaged in an amount to be determined at trial, including, but not limited to, repair and replacement costs, monetary losses

associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT XV
Violation of the MMWA
15 U.S.C. § 2301, et seq.
(On Behalf of the Florida Class)

419. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

420. This Count is brought on behalf of Plaintiff Pollack (for the purposes of this section, "Plaintiff") and the Florida Class.

421. Plaintiff and the Florida Class members satisfy the MMWA's jurisdictional requirement because this action satisfies the diversity jurisdiction requirements under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

422. Plaintiff and the members of the Florida Class are "consumers" within the meaning of the MMWA, 15 U.S.C. § 2301(3).

423. Defendant is a "supplier" and "warrantor" within the meaning of the MMWA, 15 U.S.C. § 2301(4)-(5).

424. AMD's processors are "consumer products" within the meaning of the MMWA, 15 U.S.C. § 2301(1).

425. The MMWA, 15 U.S.C. §2310(d)(1), provides a cause of action for any consumer who is damaged by the failure of a warrantor to comply with a written warranty.

426. Defendant provided Plaintiff and members of the Florida Class with one or more express warranties, which are covered under the MMWA, 15 U.S.C. § 2301(6). In connection with the purchase or lease of AMD processors, or devices containing AMD processors, Defendant directly provided warranty coverage for its processors, or indirectly provided warranty coverage for its processors under one or more manufacturer's warranties.

427. Through written advertisements, Defendant marketed its processors to the Plaintiff and members of the Florida Class as secure ***and*** of particular processing speeds. Indeed, such representations formed the basis of the bargain in Plaintiff and the Florida Class's decision to purchase or lease AMD processors, or devices containing AMD processors.

EXHIBIT 1
Page 98 of 123

428. Plaintiff and members of the Florida Class experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant, and have not been provided a suitable repair or replacement of the defective processors free of charge within a reasonable time.

429. In connection with the purchase or lease of AMD processors, or of devices containing AMD processors, Defendant breached these warranties by misrepresenting the standard, quality, or grade of its processors, and failing to disclose and fraudulently concealing the existence of the Defect in its processors. AMD processors share a common defect in design, workmanship, and manufacture that is prone to security vulnerabilities and fail to operate as represented by Defendant.

430. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors. Under the circumstances, the remedies available under any informal settlement procedure would be inadequate and any requirement that Plaintiff and the members of the Florida Class resort to an informal dispute resolution procedure and/or afford Defendant a reasonable opportunity to cure their breach of warranties is excused and thereby deemed satisfied.

431. Any attempt by Defendant to disclaim or limit its express or implied warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. Among other things, Plaintiff and members of the Florida Classes did not participate in determining any warranty limitations, especially those which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant on the one hand, and Plaintiff and members of the Florida Class on the other hand, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD

EXHIBIT 1
Page 99 of 123

processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

432. Plaintiff and members of the Florida Class would suffer economic hardship if they returned their AMD processors, or devices containing the AMD processors, but did not receive the return of all payments made by them to Defendant. Thus, Plaintiff and the Florida Class members have not reaccepted their AMD processors by retaining them

433. The amount in controversy of Plaintiff and the Florida Class's individual claims meets or exceeds the sum of $25. The amount in controversy of this action exceeds the sum of $50,000, exclusive of interest and costs, computed on the basis of all claims to be determined in this lawsuit.

434. Plaintiff and members of the Florida Class, individually and on behalf of the respective Classes, seek all damages permitted by law, including diminution in the value of the AMD processors, in an amount to be proven at trial.

COUNT XVI
Negligence
(On Behalf of the Florida Class)

435. Plaintiff no longer asserts a negligence claim.

C. Louisiana Counts

COUNT XVII
Warranty Against Redhibitory Defects
La. Civ. Code Art. 2520, 2524 (2015)
(On Behalf of the Louisiana Class)

436. Plaintiff Hauck (for the purposes of this section, "Plaintiff") realleges and incorporates by reference all preceding allegations as though fully set forth herein.

437. Plaintiff Hauck brings this Count on behalf of herself and the Louisiana Class.

438. Defendant marketed its processors to Plaintiff and the Louisiana Class as secure ***and*** of particular processing speeds. At the time of their purchase, ***the processors were not both secure and capable of reaching the advertised speeds, as represented by Defendant***. Indeed, such representations formed the basis of the bargain in Plaintiff's and the Louisiana Class's decision to purchase or lease AMD processors, or devices containing AMD processors.

EXHIBIT 1

439. Defendant's omissions caused Plaintiff and members of the Louisiana Class to be unaware at the time of their purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to their sensitive information; (iii) the AMD CPU that powered their computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerability created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered their computers to reach the advertised performance level.

440. The AMD processors were defective when they left Defendant's possession and, as such, could not perform according to Defendant's affirmative representations that the AMD processors were secure ***and*** of particular processing speeds. Moreover, developing a permanent solution to the Defect may not be possible (without upgrading the hardware) and, even if possible, will negatively impact the performance of the AMD processors or the devices containing such processors.

441. The Defect in the AMD processors render their use so inconvenient that Plaintiff and members of the Louisiana Class would not have purchased or leased the AMD processors, or devices containing AMD processors, had they known of the Defect. Accordingly, Plaintiff and the Louisiana Class are entitled to obtain a rescission of the sale of the AMD processors.

442. Alternatively, the Defect diminishes the usefulness of the AMD processors (or devices containing such processors) or their value so that Plaintiff and members of the Louisiana Class would still have bought the AMD processors (or devices containing such processors) but for a lesser price. Accordingly, Plaintiff and the Louisiana Class are entitled to obtain a reduction of the price.

443. Defendant is liable as a bad faith seller for selling a defective product with knowledge of the Defect, and thus, is liable to Plaintiff and the Louisiana Class members for the price of the AMD processors, or of the devices containing such processors, with interest from the purchase date, as well as reasonable expenses occasioned by the sale of the AMD processors, or of

the devices containing such processors, and attorneys' fees. As the manufacturer of the AMD processors, Defendant is deemed to know that the AMD processors possessed a redhibitory defect.

444. Additionally, a warranty that the AMD processors were fit for the ordinary purpose for which processors are used is implied by law pursuant to La. Civ. Code Art. 2524.

445. These AMD processors, when sold or leased and at all times thereafter, were not fit for the ordinary purpose for which processors are used.

446. Plaintiff and the Louisiana Class members seek a judgment in their favor for all possible damages, together with interest, costs herein incurred, attorneys' fees, and all such other and further relief as this Court deems just and proper.

COUNT XVIII
Violation of the MMWA
15 U.S.C. § 2301, et seq.
(On Behalf of the Louisiana Class)

447. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

448. Plaintiff brings this Count on behalf of herself and the Louisiana Class.

449. Plaintiff and the Louisiana Class members satisfy the MMWA's jurisdictional requirement because this action satisfies the diversity jurisdiction requirements under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

450. Plaintiff and the Louisiana Class members are "consumers" within the meaning of the MMWA, 15 U.S.C. § 2301(3).

451. Defendant is a "supplier" and "warrantor" within the meaning of the MMWA, 15 U.S.C. § 2301(4)-(5).

452. The AMD processors described above are "consumer products" within the meaning of the MMWA, 15 U.S.C. § 2301(1).

453. The MMWA, 15 U.S.C. § 2310(d)(1), provides a cause of action for any consumer who is damaged by, among other things, the failure of a warrantor to comply with written or implied warranties.

454. Defendant sells and leases the AMD processors subject to implied (including statutory) warranties within the meaning of the MMWA, 15 U.S.C. § 2301(7).

EXHIBIT 1
Page 102 of 123

455. Through written advertisements, Defendant marketed its processors to Plaintiff and the Louisiana Class members as secure ***and*** of particular processing speeds. Indeed, such representations formed the basis of the bargain in Plaintiff's and the Louisiana Class's decision to purchase or lease AMD processors, or devices containing AMD processors.

456. AMD processors were not secure—given that they were subject to the Defect—and did not operate at stated processing speeds, given that patches necessary to mitigate the Defect result in reduced processing performance.

457. Plaintiff and members of the Louisiana Class experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant, and have not been provided a suitable repair or replacement of the defective processors free of charge within a reasonable time.

458. Defendant provided Plaintiff and members of the Louisiana Class with one or more implied warranties, which are covered under the MMWA, 15 U.S.C. § 2301(7).

459. In connection with the purchase or lease of AMD processors, or devices containing AMD processors, Defendant breached these warranties by misrepresenting the standard, quality, or grade of its processors, and failing to disclose and fraudulently concealing the existence of the Defect in its processors. AMD processors share a common defect in design, workmanship, and manufacture that is prone to security vulnerabilities and fails to operate as represented by Defendant. The AMD processors were defective when they left Defendant's possession and, as such, could not perform according to Defendant's affirmative representations that the AMD processors were secure and of particular processing speeds. Moreover, developing a permanent solution to the Defect may not be possible (without upgrading the hardware) and, even if possible, will negatively impact the performance of the AMD processors or the devices containing such processors.

460. Plaintiff and the Louisiana Class members used Defendant's products and had business dealings with Defendant, either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

461. Defendant breached the express warranty by selling AMD processors that were defective with respect to design, workmanship, and manufacture when Defendant knew its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

462. When Plaintiff and the Louisiana Class purchased or leased the AMD processors, or devices containing such processors, Defendant warranted that the processors were fit for their ordinary purpose for which they intended to be used.

463. Defendant has breached its implied warranties by failing to disclose and repair the Defect in the AMD processors, and by selling or leasing AMD processors that are unfit for their ordinary purposes.

464. Any attempt by Defendant to disclaim or limit its express or implied warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. Among other things, Plaintiff and members of the Louisiana Class did not participate in determining any warranty limitations, especially those which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Louisiana Class, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

465. Plaintiff and members of the Nationwide and the Louisiana Class would suffer economic hardship if they returned their AMD processors, or devices containing the AMD processors, but did not receive the return of all payments made by them to Defendant. Thus, Plaintiff and members of the Louisiana Class have not reaccepted their AMD processors by retaining them.

466. The amount in controversy of Plaintiff's and the Louisiana Class's individual claims meets or exceeds the sum of $25. The amount in controversy of this action exceeds the sum of

EXHIBIT 1
Page 104 of 123

$50,000, exclusive of interest and costs, computed on the basis of all claims to be determined in this lawsuit.

467. Plaintiff and the Louisiana Class members seek all damages permitted by law, including diminution in value of their AMD processors, or devices containing such processors, in an amount to be proven at trial.

D. Massachusetts Counts

COUNT XIX
Violation of the Massachusetts Consumer Protection Act ("MCPA")
Mass. Gen. Laws 93A, § 1, et seq.
(On Behalf of the Massachusetts Class)

468. Plaintiff Caskey-Medina (for the purposes of this section, "Plaintiff") realleges and incorporates by reference all preceding allegations as though fully set forth herein.

469. Plaintiff brings this Count on behalf of himself and the Massachusetts Class.

470. Defendant, Plaintiff, and members of the Massachusetts Class are "persons" within the meaning of Mass. Gen. Laws 93A, § 1(a).

471. Defendant engaged in "trade" or "commerce" within the meaning of Mass. Gen. Laws 93A, § 1(b).

472. The MCPA prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." Mass. Gen. Laws 93A, § 2(a).

473. In the course of its business, Defendant violated the MCPA by misrepresenting the performance and security capabilities and features of its processors, and failing to disclose and omitting the existence of the Defect in its processors. As such, Defendant violated the Massachusetts Act by:

(a) representing that the AMD processors have characteristics, uses, benefits, or qualities that they do not have;

(b) representing that the AMD processors are of a particular standard, quality, and grade when they are not; and/or

(c) advertising the AMD processors with the intent not to sell them as advertised.

474. Defendant failed to disclose and omitted the existence of the Defect in its processors. Defendant's omissions caused Plaintiff and members of the Massachusetts Class to be unaware at the time of their purchase that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to their sensitive information; (iii) the AMD CPU that powered their computer could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerability created by the Defect; and (v) attempts to "patch" the Defect would prevent the AMD CPU that powered their computers to reach the advertised performance level.

475. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiff and members of the Massachusetts Class, but failed to do so. Defendant had a duty to disclose that the AMD processors were defective because, having volunteered to provide information to Plaintiff and the Massachusetts Class regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure ***and*** capable of reaching the advertised speeds. Further, knowledge of the existence of the Defect was in the superior control of Defendant.

476. Defendant's scheme and concealment of the true characteristics of the AMD processors was material to Plaintiff and members of the Massachusetts Class. The Defect relates to the central functionality of the AMD processors as it affects the processors' ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information. Plaintiff and members of the Massachusetts Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

477. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiff and the Massachusetts Class, Defendant had the duty to disclose not just the partial truth, but the entire truth.

478. Defendant intentionally and knowingly failed to disclose and misrepresented material facts regarding the AMD processors with intent to mislead Plaintiff and members of the Massachusetts Class.

479. Defendant's deceptive conduct was likely to deceive a reasonable consumer, and did in fact deceive reasonable consumers including Plaintiff and members of the Massachusetts Class.

480. Plaintiff and members of the Massachusetts Class reasonably relied upon Defendant's material omissions and misrepresentations. They had no way of knowing that Defendant's representations were false and misleading. Plaintiff and members of the Massachusetts Class did not (and could not) unravel Defendant's deception on their own.

481. The facts concealed and omitted by Defendant from Plaintiff and members of the Massachusetts Class are material in that a reasonable consumer would have considered them to be important in deciding whether to purchase or lease the AMD processors (or devices containing AMD processors) or pay a lower price. Had Plaintiff and members of the Massachusetts Class known about the defective nature of AMD processors, they would not have purchased or leased the AMD processors (or devices containing AMD processors), or would not have paid the prices they paid.

482. Plaintiff and members of the Massachusetts Class suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's conduct. Pursuant to Mass. Gen. Laws 93A, § 9, Plaintiff and members of the Massachusetts Class seek monetary relief against Defendant measures as the greater of (a) actual damages in an amount to be determined at trial and (b) statutory damages in the amount of $25 for Plaintiff and each member of the Massachusetts Class. Because Defendant's conduct was committed willfully and knowingly, Plaintiff and members of the Massachusetts Class are entitled to recover, for Plaintiff and each member of the Massachusetts Class, up to three times actual damages, but no less than two times actual damages.

483. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. In addition, on June 14, 2018, a notice letter was sent on behalf of Plaintiff and the members of the Massachusetts Class to Defendant, attached hereto as **Exhibit B**. Defendant has not responded to this notice.

COUNT XX
Fraud by Omission
(On Behalf of the Massachusetts Class)

484. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

485. This Count is brought on behalf of Plaintiff and the Massachusetts Class.

486. Defendant intentionally and knowingly omitted material facts about its AMD processors, including the fact that the processors have significant security vulnerabilities and that the advertised processer speeds were not available without rendering the processors vulnerable to side-channel attacks, which expose users' private information to potential hacking through such side-channel attacks.

487. Defendant acted with the intent that Plaintiff and members of the Massachusetts Class rely on Defendant's omissions so that Defendant could profit from the sale of the processors.

488. Specifically, Defendant's fraudulent omissions include, but are not limited to:

(a) selling or leasing the AMD processors, either directly or as a component of devices containing such processors, to Plaintiffs and members of the Massachusetts Class, either directly or indirectly through third parties, with knowledge of the Defect in the AMD processors, and failing to disclose that: (i) the Defect existed; (ii) the Defect allowed an attacker to gain access to Plaintiff's and members of the Massachusetts Class' sensitive information; (iii) the AMD CPU that power their computers could not reach the advertised performance level without relying on defectively designed CPU microarchitecture components that compromised the security of their sensitive information; (iv) the security technologies AMD made available to consumers did not address the security vulnerabilities created by the Defect;;

(b) omitting the fact in Defendant's public statements, statements to third-party retailers, and on the packaging of its processors that AMD processors were capable achieving particular speeds only if the data of Plaintiffs and members of the

Massachusetts Class were made vulnerable to side-channel attacks, with the intent that those statements and omissions be relied upon;

(c) making public statements and statements to third-party retailers regarding the security of AMD processors in tandem with the previously described omissions in order to conceal the Defect and its corresponding security risk from Plaintiff and members of the Massachusetts Class; and/or

(d) failing to disclose that AMD processors were vulnerable to the Defect and only disclosing that fact publicly on January 11, 2018.

489. Defendant's statements and omissions regarding the speed and/or security of its processors were objectively verifiable statements or omissions of fact, and not mere puffery.

490. The who, what, where, and why of Defendant's fraudulent business practices are as follows:

(a) **Who**: Defendant AMD;

(b) **What**: Defendant affirmatively omitted the fact there are significant security vulnerabilities with the processors and that the speed of its processors was only available if consumers' data was left vulnerable by representing that its processors were both secure ***and*** capable of reaching particular speeds;

(c) **Where**: Defendant omitted the existence of the Defect from Plaintiffs and members of the Massachusetts Class on its packaging for its processors, on the packaging by third-party computer and server manufacturers, on in-store or online displays communicated to retailers by AMD or its authorized retailers (e.g. Fry's, Newegg.com); and/or

(d) **Why**: Because, contrary to AMD's omissions, AMD processors are not secure and are only capable of working at the speed and with the performance as promised at the expense of a significant security vulnerability. Instead, AMD processors are either partially secure ***or*** capable of working at the speed promised.

491. Defendant was provided notice of the Defect by independent research teams no later than June 2017, and knew of the existence of the Defect much earlier. Nevertheless, Defendant

failed to disclose the existence of the Defect in its processors. Defendant owed a duty to disclose the material fact that its processors were defective to Plaintiff and members of the Massachusetts Class, but failed to do so. Defendant had a duty to disclose that the AMD processors were defective, because, having volunteered to provide information to Plaintiff and the Massachusetts Class regarding the security of the processors, Defendant had a duty to disclose not just the partial truth, but the entire truth: that contrary to Defendant's representations, the processors were not both secure ***and*** capable of reaching the advertised speeds. Further, knowledge of the existence of the Defect was in the superior control of Defendant.

492. Defendant owed a duty to disclose the Defect in its processors because Defendant did not disclose that the advertised speeds for AMD processors were only available at the expense of a significant security vulnerability, which constitutes a partial disclosure. Rather than disclose the Defect, Defendant intentionally and knowingly omitted materials facts including the existence of the Defect and that the represented processor speeds were only available at the expense of a significant security vulnerability in order to deceive consumers and sell additional processors and avoid the cost of repair or replacement of the defective processors.

493. Defendant's fraudulent acts were likely to deceive a reasonable consumer. Plaintiff and members of the Massachusetts Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors.

494. Defendant's scheme and failure to disclose the true characteristics of the AMD processors were material to Plaintiff and members of the Massachusetts Class as evidence by, among other things, the massive public outcry once the Defect was disclosed. Moreover, the Defect relates to the central functionality of the AMD processors as it affects the processor's ability to ensure effective and efficient performance of a computer or similar device, and to maintain sufficient data security to adequately process, communicate, and store sensitive and confidential information. Defendant knew its omissions were misleading and knew the effect of those omissions.

EXHIBIT 1

495. Defendant failed to disclose the truth with the intention that Plaintiff and members of the Massachusetts Class would rely on the omissions. Had they known the truth, Plaintiff and members of the Massachusetts Class would not have purchased or leased, or would have paid significantly less for, AMD processors, or devices containing AMD processors.

496. As a direct and proximate result of Defendant's failure to disclose material information, Plaintiff and members of the Massachusetts Class have suffered actual damages, in an amount to be proven at trial.

COUNT XXI
Breach of Express Warranty – Limited Warranty
Mass. Gen. Laws 106, § 2-313, et seq.
(On Behalf of the Massachusetts Class)

497. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

498. Plaintiff brings this Count on behalf of himself and the Massachusetts Class.

499. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Mass. Gen. Laws . 106 § 2-104(1), and a "seller" of the AMD processors under Mass. Gen. Laws 106 § 2-103(1)(d).

500. The AMD processors are and were at all relevant times "goods" within the meaning of MASS. GEN. LAWS ch. 106 § 2-105(1).

501. In connection with the purchase of AMD processors sold through the AMD Processor in a Box program, AMD provided a three-year limited warranty for processors sold with a heatsink/fan ("HSF") and a two-year limited warranty for processors sold without an HSF. Both warranties cover defects in the material and workmanship of the AMD processors, and processors that fail to substantially conform to AMD's publicly available specifications.

502. Plaintiff and members of the Massachusetts Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors. As such, Defendant's express warranty regarding the benefits of the AMD processors extends directly to consumers like Plaintiff and members of the Massachusetts Class, who are intended third-party beneficiaries of any contract between Defendant and the retailers where AMD processors, or devices with AMD processors, were sold or leased.

503. Plaintiff and members of the Massachusetts Class experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant.

504. Plaintiff and the Massachusetts Class could not have reasonably discovered the Defect in AMD processors prior to the public disclosure of the Defect by cybersecurity experts or prior to experiencing a known security hack resulting from the Defect.

505. Defendant breached the express warranty by selling AMD processors that were defective with respect to design, workmanship, and manufacture when Defendant knew its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

506. Because of the existence of the Defect, the AMD processors do not perform as warranted.

507. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

508. Thus, Defendant's two-year and three-year limited warranties fail of their essential purpose and the recovery of Plaintiff and members of the Massachusetts Class is not limited to the remedies of the express limited warranties.

509. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. This reasoning equally applies to any attempt to limit the warranties Defendant furnished directly to Plaintiff and members of the Massachusetts Class through its marketing campaign, regardless of whether Plaintiff and members of the Massachusetts Class

purchased or leased their AMD processors, or devices containing such processors, through the AMD Processor in a Box program.

510. Furthermore, the time limits contained in the express limited warranties Defendant furnished in connection with the AMD Processor in a Box program were also unconscionable and inadequate to protect Plaintiff and members of the Massachusetts Class. Among other things, Plaintiff and members of the Massachusetts Class did not determine these limitations, the terms of which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Massachusetts Class, and Defendant knew known that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

511. Defendant knew that its processors were inherently defective and did not conform to their warranties. Plaintiff and members of the Massachusetts Class were induced into purchasing or leasing AMD processors, or devices containing AMD processors, under false pretenses.

512. Plaintiff and members of the Massachusetts Class have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

513. As a direct and proximate result of Defendant's breach of express warranties, Plaintiff and members of the Massachusetts Class have been damaged in an amount to be determined at trial, including, but not limited to, repair and replacement costs, monetary losses associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT XXII
Breach of Express Warranty – Representations
Mass. Gen. Laws 106, § 2-313.
(On Behalf of the Massachusetts Class)

514. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

515. Plaintiff brings this Count on behalf of himself and the Massachusetts Class.

EXHIBIT 1

516. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Mass. Gen. Laws 106 § 2-104(1), and a "seller" of the AMD processors under Mass. Gen. Laws 106 § 2-103(1)(d).

517. The AMD processors are and were at all relevant times "goods" within the meaning of Mass. Gen. Laws 106 § 2-105(1).

518. Defendant marketed its processors to Plaintiff and the members of the Massachusetts Class, and made affirmative representations, as to the security ***and*** processing speeds of the processors. The affirmative representations purposefully omitted mention of the Defect or that the speed of the processors was only possible as a result of the Defect, which users' sensitive data exposed. At the time of their purchase, ***the processors were not both secure and capable of reaching the advertised speeds, as represented by Defendant***. Plaintiff and members of the Massachusetts Class were exposed to, and aware of, these representations.

519. Defendant's express warranties formed the basis of the bargain in Plaintiff's and the Massachusetts Class's decision to purchase or lease AMD processors, or devices containing AMD processors. Defendant's various oral and written representations regarding the AMD processors' security and processing speed constituted express warranties to Plaintiff and the Massachusetts Class.

520. An affirmation of fact, promise, or description made by the seller to the buyer which relates to the goods and becomes a part of the basis of the bargain creates an express warranty that the goods will conform to the affirmation, promise, or description.

521. Plaintiff and members of the Massachusetts Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors. As such, Defendant's express warranty regarding the benefits of the AMD processors extends directly to consumers like Plaintiff and members of the Massachusetts Class, who are intended third-party beneficiaries of any contract between Defendant and the retailers where AMD processors, or devices with AMD processors, were sold or leased.

522. Defendant represented that its processors were secure ***and*** of particular processing speeds. AMD processors were not secure—given that they were subject to the Defect—and did not

operate at stated processing speeds, given that patches necessary to mitigate the Defect result in reduced processing performance.

523. Plaintiff and members of the Massachusetts Class experienced the existence of the Defect in AMD processors but had no knowledge of the existence of the Defect, which was known and concealed by Defendant.

524. Plaintiff and the Massachusetts Class could not have reasonably discovered the Defect in AMD processors prior to the public disclosure of the Defect by cybersecurity experts or prior to experiencing a known security hack resulting from the Defect.

525. Because of the existence of the Defect, the AMD processors do not perform as warranted.

526. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

527. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. This reasoning equally applies to any attempt to limit the warranties Defendant furnished directly to Plaintiff and members of the Massachusetts Class through its marketing campaign, regardless of whether Plaintiff and members of the Massachusetts Class purchased or leased their AMD processors, or devices containing such processors, through the AMD Processor in a Box program.

528. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Massachusetts Class, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its

processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

529. Defendant knew that its processors were inherently defective and did not conform to their warranties. Plaintiff and members of the Massachusetts Class were induced into purchasing or leasing AMD processors, or devices containing AMD processors, under false pretenses.

530. Plaintiff and members of the Massachusetts Class have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

531. As a direct and proximate result of Defendant's breach of express warranties, Plaintiff and members of the Massachusetts Class have been damaged in an amount to be determined at trial, including, but not limited to, repair and replacement costs, monetary losses associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT XXIII
Breach of Implied Warranty
Mass. Gen. Laws 106, §§ 2-314, 2-315, et seq.
(On Behalf of the Massachusetts Class)

532. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

533. Plaintiff brings this Count on behalf of himself and the Massachusetts Class.

534. Defendant is and was at all relevant times a "merchant" with respect to the AMD processors under Mass. Gen. Laws 106 § 2-104(1), and a "seller" of the AMD processors under Mass. Gen. Laws § 2-103(1)(d).

535. The AMD processors are and were at all relevant times "goods" within the meaning of Mass. Gen. Laws 106 § 2-105(1).

536. A warranty that the AMD processors were in merchantable condition and fit for their ordinary purpose is implied by law pursuant to Mass. Gen. Laws 106 § 2-314.

537. Defendant knew at the time of sale of the AMD processors that Plaintiff and members of the Massachusetts Class intended to use those processors in an ordinary manner by providing basic security for their sensitive data, and that Plaintiff and members of the

Massachusetts Class were relying on Defendants' skill and judgment to furnish suitable products for this ordinary purpose.

538. Plaintiff and members of the Massachusetts Class purchased or leased AMD processors, or devices containing AMD processors, from Defendant, by and through Defendant's authorized agents for retail sales, or were otherwise expected to be the eventual purchasers or lessors of AMD processors when purchased or leased from a third party. At all relevant times, Defendant was the manufacturer, distributor, warrantor, and/or seller of the relevant processors. Defendant knew of the specific use for which its processors were purchased or leased.

539. AMD processors, when sold or leased and at all times thereafter, were not in merchantable condition and were not fit for the ordinary purpose due to the Defect, and the associated problems and failures caused by the Defect. Thus, Defendant breached its implied warranty of merchantability.

540. Plaintiff and members of the Massachusetts Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third parties, and were the intended recipients of Defendant's processors. As such, Defendant's implied warranty regarding the benefits of the AMD processors extends directly to consumers like Plaintiff and members of the Massachusetts Class, who are intended third-party beneficiaries of any contract between Defendant and the retailers where AMD processors, or devices with AMD processors, were sold or leased.

541. Defendant marketed its processors to Plaintiff and members of the Massachusetts Class as secure and of particular processing speeds. Plaintiff and members of the Massachusetts Class were exposed to, and aware of, these representations. Indeed, such representations formed the basis of their respective decisions to purchase or lease AMD processors, or devices containing AMD processors.

542. The AMD processors were defective when they left Defendant's possession because they were not both secure ***and*** capable of achieving their particular, advertised processing speeds, and, as such, could not perform according to Defendant's affirmative representations that the AMD processors were secure and of particular processing speeds. Therefore, the AMD processors were not reasonably fit for their intended, anticipated, or reasonably foreseeable use.

EXHIBIT 1

543. As a direct and proximate result of Defendant's breach of its implied warranty of merchantability, Plaintiff and members of the Massachusetts Class have been damaged in an amount to be proven at trial.

544. Defendant cannot disclaim its warranties implied by law as it knowingly sold or leased a defective product.

545. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of implied warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors.

546. Any attempt by Defendant to disclaim or limit the implied warranty of merchantability vis-à-vis Plaintiff and members of the Massachusetts Class is unconscionable and unenforceable. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. Among other things, Plaintiff and members of the Massachusetts Class did not participate in determining any warranty limitations, especially those which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Massachusetts Class, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

547. Further, as a manufacturer of consumer goods, Defendant is precluded from excluding or modifying an implied warranty of merchantability or limiting customers' remedies for breach of this warranty.

548. Plaintiff and members of the Massachusetts Class have complied with all obligations under the warranty, or otherwise have been excused from performance of said obligations as a result of Defendant's conduct described herein.

549. Defendant's warranties were designed to influence consumers who purchased or leased its processors, including products that contain them.

550. Defendant is estopped by its conduct, as alleged herein, from disclaiming any and all implied warranties with respect to the defective processors.

551. The applicable statute of limitations for the implied warranty claim has been tolled by the discovery rule and Defendant's concealment.

COUNT XXIV
Violation of the MMWA,
15 U.S.C. § 2301, et seq.
(On Behalf of the Massachusetts Class)

552. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

553. Plaintiff brings this Count on behalf of himself and the Massachusetts Class.

554. Plaintiff and members of the Massachusetts Class satisfy the MMWA's jurisdictional requirement because this action satisfies the diversity jurisdiction requirements under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

555. Plaintiff and members of the Massachusetts Class are "consumers" within the meaning of the MMWA, 15 U.S.C. § 2301(3).

556. Defendant is a "supplier" and "warrantor" within the meaning of the MMWA, 15 U.S.C. § 2301(4)-(5).

557. AMD's processors are "consumer products" within the meaning of the MMWA, 15 U.S.C. § 2301(1).

558. The MMWA, 15 U.S.C. § 2310(d)(1), provides a cause of action for any consumer who is damaged by the failure of a warrantor to comply with a written or implied warranties.

559. Defendant provided Plaintiff and members of the Massachusetts Class with one or more express warranties, which are covered under the MMWA, 15 U.S.C. § 2301(6). In connection with the purchase or lease of AMD processors, or devices containing AMD processors, Defendant directly provided warranty coverage for its processors, or indirectly provided warranty coverage for its processors under one or more manufacturer's warranties.

EXHIBIT 1
Page 119 of 123

560. Through written advertisements, Defendant marketed its processors to the Plaintiff and members of the Massachusetts Class as secure and of particular processing speeds. Indeed, such representations formed the basis of the bargain in Plaintiff's and members of the Massachusetts Class's decision to purchase or lease AMD processors, or devices containing AMD processors.

561. Plaintiff and members of the Massachusetts Class experienced the existence of the Defect in AMD processors within the warranty periods but had no knowledge of the existence of the Defect, which was known and concealed by Defendant, and have not been provided a suitable repair or replacement of the defective processors free of charge within a reasonable time.

562. Defendant provided Plaintiff and members of the Massachusetts Class with one or more implied warranties, which are covered under the MMWA, 15 U.S.C. § 2301(7).

563. In connection with the purchase or lease of AMD processors, or devices containing AMD processors, Defendant breached these warranties by misrepresenting the standard, quality, or grade of its processors, and failing to disclose and fraudulently concealing the existence of the Defect in its processors. AMD processors share a common defect in design, workmanship, and manufacture that is prone to security vulnerabilities and fails to operate as represented by Defendant.

564. Defendant was provided notice of the Defect by independent research teams, and knew of the existence of the Defect much earlier. Affording Defendant a reasonable opportunity to cure its breach of warranties would be unnecessary and futile here because Defendant has known of and concealed the Defect and has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defect's existence at the time of sale or lease of the processors, or devices containing AMD processors. Under the circumstances, the remedies available under any informal settlement procedure would be inadequate and any requirement that Plaintiff and members of the Massachusetts Class resort to an informal dispute resolution procedure and/or afford Defendant a reasonable opportunity to cure their breach of warranties is excused and thereby deemed satisfied.

565. Any attempt by Defendant to disclaim or limit its express or implied warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is

EXHIBIT 1
Page 120 of 123

unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defect. Among other things, Plaintiff and members of the Massachusetts Class did not participate in determining any warranty limitations, especially those which unreasonably favor Defendant. A gross disparity in bargaining power existed between Defendant and Plaintiff and members of the Massachusetts Class, and Defendant knew that its processors were defective at the time of sale or lease of the processors, or devices containing AMD processors, and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

566. Plaintiff and members of the Massachusetts Class would suffer economic hardship if they returned their AMD processors, or devices containing the AMD processors, but did not receive the return of all payments made by them to Defendant. Thus, Plaintiff and members of the Massachusetts Class have not reaccepted their AMD processors by retaining them.

567. The amount in controversy of Plaintiff and members of the Massachusetts Class's individual claims meets or exceeds the sum of $25. The amount in controversy of this action exceeds the sum of $50,000, exclusive of interest and costs, computed on the basis of all claims to be determined in this lawsuit.

568. Plaintiff and members of the Massachusetts Class, individually and on behalf of the respective Classes, seek all damages permitted by law, including diminution in the value of the AMD processors, in an amount to be proven at trial.

COUNTXXV
Negligence
(On Behalf of the Massachusetts Class)

569. Plaintiff no longer asserts a negligence claim.

VIII. PRAYER FOR RELIEF

570. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request that this Court enter judgment against Defendant and in favor of Plaintiffs and the Classes, and award the following relief:

(a) An order certifying this action as a class action pursuant to Rule 23 of the Fed. R. Civ. P., declaring Plaintiffs as the representatives of the Classes, and Plaintiffs' counsel as counsel for the Classes;

(b) An order awarding declaratory relief and enjoining Defendant from continuing the unlawful, deceptive, harmful, and unfair business conduct and practices alleged herein;

(c) Appropriate injunctive and equitable relief;

(d) A declaration that Defendant is financially responsible for all Class notice and the administration of Class relief;

(e) Costs, restitution, damages, including statutory and punitive damages, penalties, and disgorgement in an amount to be determined at trial;

(f) An order requiring Defendant to pay both pre- and post-judgment interest on any amounts awarded;

(g) An award of costs and attorneys' fees; and

(h) Such other or further relief as the Court may deem appropriate, just, and equitable.

IX. DEMAND FOR JURY TRIAL

571. Plaintiffs hereby demand a trial by jury.

DATED: December 6, 2018

Respectfully submitted,

ROBBINS GELLER RUDMAN & DOWD LLP

/s/Stuart A. Davidson
STUART A. DAVIDSON (*Pro Hac Vice*)
sdavidson@rgrdlaw.com
RICARDO J. MARENCO (*Pro Hac Vice*)
rmarenco@rgrdlaw.com
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Tel: (561) 750-3000
Fax: (561) 750-3364

-and-

ROBERT M. ROTHMAN (*Pro Hac Vice*)
rrothman@rgrdlaw.com
58 South Service Road, Suite 200
Melville, NY 11747
Tel: (631) 367-7100
Fax: (631) 367-1173

KESSLER TOPAZ
MELTZER & CHECK, LLP
JENNIFER L. JOOST (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Tel: (415) 400-3000
Fax: (415) 400-3001

- and –

JOSEPH H. MELTZER (*Pro Hac Vice*)
jmeltzer@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610) 667-7056

Interim Co-Lead Plaintiffs' Counsel